



TheGreenBow Cliente VPN IPSec

Manual de Usuario

Contacto: support@thegreenbow.es

Website: www.thegreenbow.es

Cliente VPN IPSec TheGreenBow - Manual de Usuario

Impreso en San Francisco August 2008.

Tabla de Contenidos



Introducción al Cliente VPN IPSec TheGreenBow

1 Introducción al Cliente VPN IPSec TheGreenBow

1.1 ¿Qué es el Cliente VPN IPSec TheGreenBow?

El Cliente VPN IPSec TheGreenBow es un programa de VPN IPSec, compatible con todas las versiones de Windows, que permite establecer conexiones seguras vía Internet generalmente entre un usuario remoto y el sistema Intranet de la Compañía. IPSec es el modo más seguro de conectarse a una empresa ya que permite una autentificación fuerte del usuario, una fuerte encriptación de la transmisión de datos y permite integrarse a la red y a la configuración de firewall existentes.
El Cliente VPN IPSec TheGreenBow es el resultado de muchos años de experiencia e investigación en seguridad de redes y en el desarrollo del controlador de redes de Windows.
El Cliente VPN IPSec completa nuestra gama de productos de seguridad en empresas. Como todos nuestros productos, es extremadamente fácil de usar e instalar.

1.2 Solución VPN Multi Gateway

El objetivo de TheGreenBow es soportar tantas gateways VPN y vendedores de dispositivos como sea posible, disponibles en el mercado para ofrecer una verdadera solución multi vendedor a sus clientes. En nuestros laboratorios, estamos continuamente probando nuevas gateways o especializaciones VPN IPSec, por lo que lista completa de gateways compatibles disponible en nuestra página web, aumenta constantemente, así que no dude en comprobar regularmente nuevas gateways VPN compatibles.

1.3 Multi USB Token and SmartCard solution

Hay muchos Tokens USB y Tarjetas inteligentes disponibles en el mercado. Es nuestra misión soportar el mayor número de fabricantes de Token USB y Tarjetas Inteligentes como sea posible, con el fin de ofrecer una verdadera solución multi vendedor a nuestros clientes. Nuevos dispositivos Token USB y SmartCard son probados en nuestros laboratorios. La lista de Tokens USB compatibles está disponible en nuestra página web y está aumentando día a día, por lo tanto, no dude en volver de forma regular para comprobar nuevos Tokens USB certificados.

En caso de que su token USB no aparece en la lista, póngase en contacto con nuestro Soporte Técnico y vamos a trabajar con usted para certificar el Token USB o la Tarjeta Inteligente.

1.4 Soporte de Dispositivos Linux

TheGreenBow soporta diferentes implementaciones VPN IPSec para Linux como StrongS/WAN y FreeS/WAN. Por ello, el Cliente VPN IPSec TheGreenBow es compatible con la mayoría de los routers y dispositivos basados en estas implementaciones para Linux. En un futuro ofreceremos más soporte en este tipo de implementaciones. Puede consultar la lista de los dispositivos VPN Linux en nuestra página web.

1.5 Características del Cliente VPN IPSec TheGreenBow

Versiones de Windows	Win2000, WinXP, Vista (32bit)
Idiomas	Alemán, Chino (simplificado), Esloveno, Español, Finlandés, Francés, Griego, Holandés, Inglés, Italiano, Japonés, Polaco, Portugués, Ruso, Serbio y Turco.
Modo de Conexión	Funciona tanto en modo VPN peer-to-peer como "punto a múltiples gateway", sin una gateway o servidor. Soporta todos los tipos de conexión como Dial-up, DSL, Cable, GSM/GPRS y WiFi. Permite conexión Rango del IP. Puede arrancar en una sesión (Remote Desktop connection).
Protocolo Tunneling	Soporte IKE completo: Nuestra implementación de IKE se basa en la implementación de OpenBSD 3.1 (ISAKMPD), ofreciendo así la mejor compatibilidad con los routers IPSec existentes.. Soporte IPSec completo: • Modo Principal y Modo Agresivo • Algoritmos de hash MD5 y SHA • Cambio de Puerto IKE
NAT Traversal	NAT Traversal Draft 1 (avanzado), Draft 2 and 3 (full implementation) • Incluye soporte de NAT_OA • Incluye NAT keepalive • Incluye NAT T Modo Agresivo NAT-Traversal en Modo Forzado.
Encriptación	Soporte varios algoritmo de encriptacíon: • 3DES, DES y AES 128/192/256bits. • Soporte de Grupos 1, 2, 5 y 14 (i.e. 768, 1024, 1536 and 2048).
Autentificación del Usuario	• Soporte X-AUTH • Soporte de PreShared keys (Claves compartidas) y Certificados X509. Compatible con la mayoría de los Routers VPN • Soporte de USB Token y SmartCard (Tarjetas Inteligentes) • Soporte flexible de Certificados: PEM, PKCS#12... Los certificados PKCS#12 se pueden importar directamente de la interfaz de usuario. Possibilidad de configurar un Certificado por tunel. • Soporte de la Autentificación en Modo Híbrido.
Detección de Punto Inactivo (DPD)	DPD es una extensión del Protocolo de Intercambio de Claves por Internet (IKE) (por ejemplo RFC3706) que permite´detectar un punto IKE inactivo.
Redundant Gateway	Gateway Redundante ofrece a los usuarios remotos una conexión segura y fiable a la red de la empresa. Las características de una Gateway Redundante permiten que el Cliente VPN TheGreenBow pueda abrir un túnel IPSec con una gateway alternativa si la principal puerta se ha caído o no responde.
Mode Config	"Mode Config" es un Intercambio de Claves por Internet (IKE) que permite a la gateway VPN IPSec aportar la configuración LAN al usuario remoto (Cliente VPN IPSec). Con el Mode Config, el usuario final puede dirigirse a todos los servidores de la red remota usando sus respectivos nombres de red (e.g. //myserver/marketing/budget) en lugar de su Dirección IP.
Memoria USB	Las configuraciones VPN y los elementos de seguridad (certificados, preshared key…) pueden guardarse en una Memoria USB para eliminar de un ordenador la información de seguridad, como una autentificación. Abre y cierra túneles de manera automática al insertar o extraer la Memoria USB.
Tarjetas Inteligentes y	El Cliente VPN IPSec TheGreenBow puede leer Certificados desde

Token USB	Tarjetas Inteligentes para explotar tarjetas de identificación de la empresa o tarjetas de empleados que puedan tener credenciales Digitales.
Consola de Registro	Todos los mensajes de las fases se registran para facilitar los tests y las fases de desarrollo. .
Interfaz de Usuario flexible	Instalación silenciosa e interfaz gráfica oculta permiten que los Informáticos desplieguen soluciones que garanticen que el usuario no modifica la configuración De este modo, el Panel de Conexión puede estar oculto, y el acceso al Panel de Configuración puede estar denegado o protegido por contraseña Drag & drop Configuraciones VPN en el Cliente VPN IPSec. Múltiples accesos directos del teclado disponibles para un uso más sencillo del Cliente VPN IPSec
Scripts	Pueden abrirse scripts o aplicaciones automáticamente antes o después de abrir un túnel, o antes o después de cerrar un túnel, por ejemplo.
Gestión de la Configuración	Interfaz de Usuario y Línea de Comandos. Configuración VPN protegida por contraseña. Puede proporcionar una configuración VPN específica sin instalación. Configuración VPN incrustada para ser testeada y depurada con los servidores TheGreenBow online.
Live update	Puede verificar actualizaciones online.
Licensing	Licencias Definitivas, Temporales o basadas en el número de versión.

1.6 OEM y Customización del Programa

Nuestra oferta se dirige especialmente a los clientes de constructores OEM e integradores de soluciones VPN globales. Proporcionamos soluciones del Cliente VPN totalmente funcionales para satisfacer así las demandas existentes. Nuestro Cliente VPN IPSec puede ser registrado como una nueva marca.

Parte



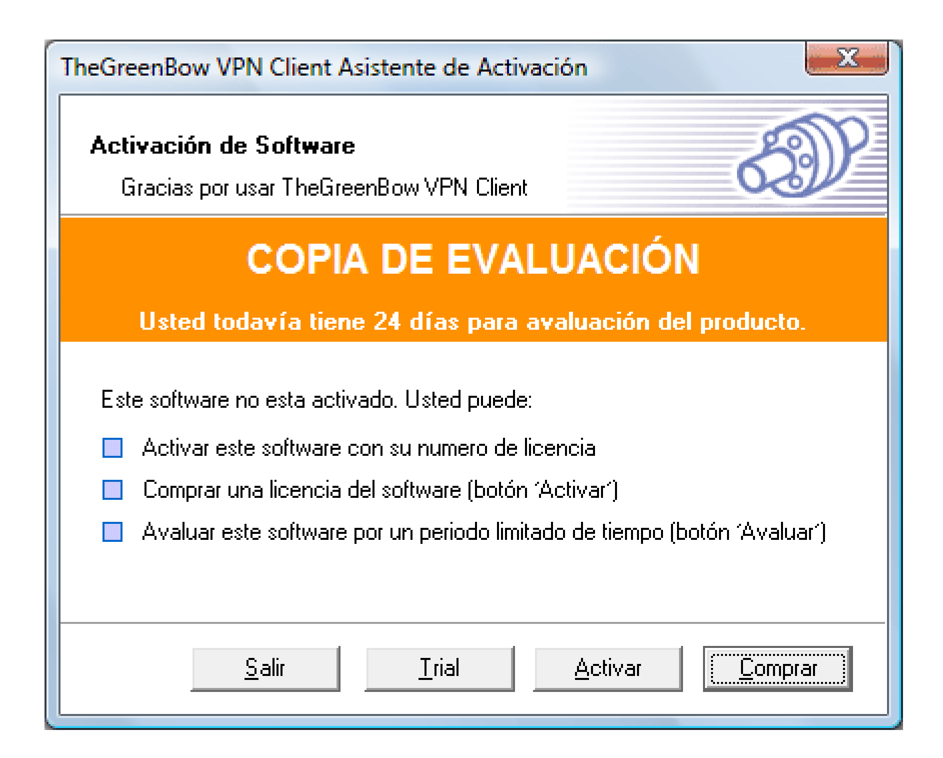
Instalar el Cliente VPN IPSec TheGreenBow

2 Instalar el Cliente VPN IPSec TheGreenBow

2.1 Instalación del Programa

La instalación del Cliente VPN TheGreenBowes una instalación clásica en Windows que no requiere información específica. Tras completar la instalación, se le preguntará si desea reiniciar su ordenador.
Tras reiniciar y entrar en la sesión, le aparecerá una ventana con varias opciones:

- “Salir” cerrará la ventana y el programa.
- "Probar' le permite continuar con la evaluación del software. El período de evaluación aparecerá en la barra naranja.
- "Activar' le permite activar el software online. Esta etapa necesita un Número de Licencia. Si hace clic en el botón “Activar”, aparecerá un Asistente de Activación.
- “Comprar” le permite comprar una Licencia de Software en la tienda online TheGreenBow online.



Atención: En Windows NT, 2000 y XP, la instalación tiene que hacerse en modo Administrador. Si no es el caso, la instalación se detendrá tras la elección del idioma con un mensaje de error.

Accesos directos: Después de instalar el programa, ya tiene acceso al Cliente VPN TheGreenBow:

- desde el escritorio, haciendo doble clic en el acceso directo TheGreenBow VPN
- desde el icono Cliente VPN de la barra de herramientas
- desde el menú Inicio > Programas > TheGreenBow > TheGreenBow VPN > TheGreenBow Cliente VPN

Nota: La Instalación del programa puede personalizarse con diversas opciones de parámetros en línea de comandos. Para más detalles, por favor diríjase al documento "Guía de Despliegue" disponible en nuestra página web.

2.1.1 Derechos de acceso

Un usuario puede tener derechos de acceso restringido a un determinado ordenador con Windows. Aquí está lo que los usuarios pueden tener acceso:

Acciones	Admin	Users
Instalación del software	sí	no
Activación del software	sí	sí
Utilización del software	sí	sí

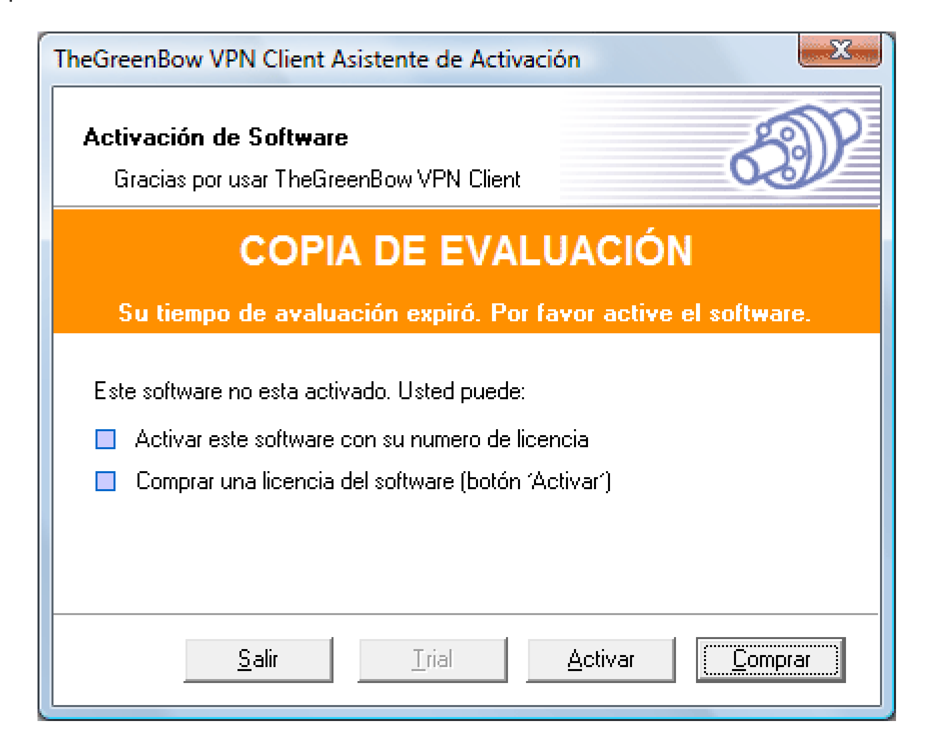
Para hacer aún más fácil, el Cliente VPN IPSec TheGreenBow crea nuevas reglas en el Firewall de Windows Vista a fin de activar el tráfico VPN IPsec. Aquí están las reglas del cortafuego de Windows Vista:

Nombre de la regla en Firewall Vista	Acción
tgbphase1	permite UDP 500
tgbphase2	permite UDP 4500

2.2 Evaluación del Programa

Es posible utilizar el Cliente VPN IPSec TheGreenBow durante el período de evaluación (limitado a 30 días de utilización) haciendo clic en el botón “Evaluación”. Cuando el Cliente VPN IPSec está en modo “Evaluación”, la ventana de registro aparece cada vez que inicie el Cliente VPN IPSec. El período de evaluación aparece en la barra naranja.

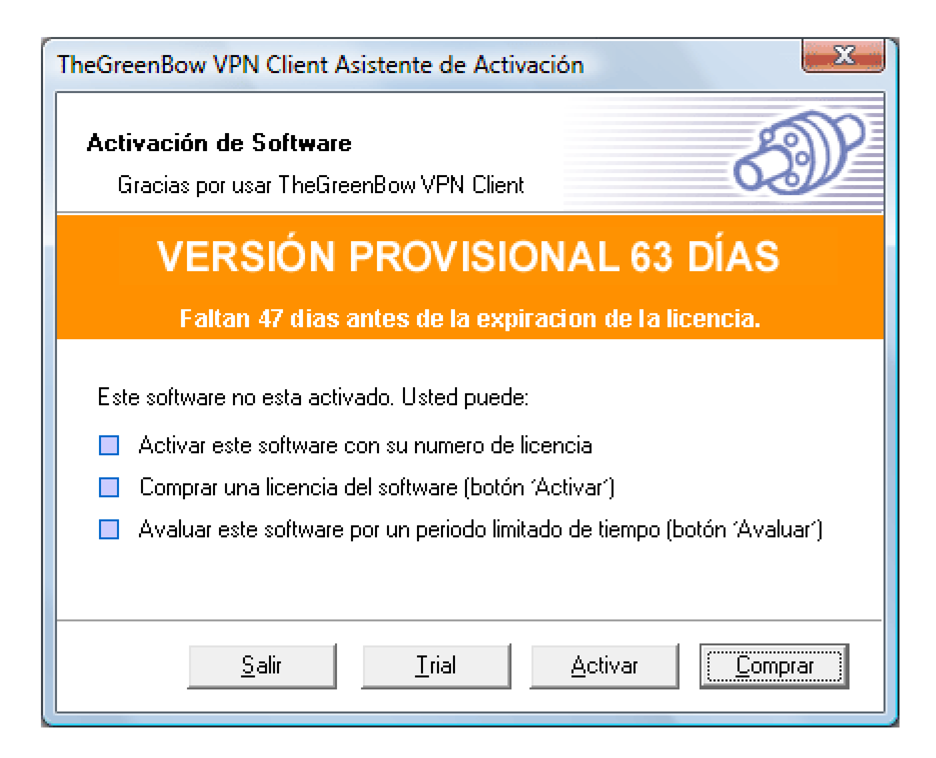
Una vez que el período de evaluación expire, el botón “Evaluación” ya no estará disponible y el software aparecerá inaccesible.



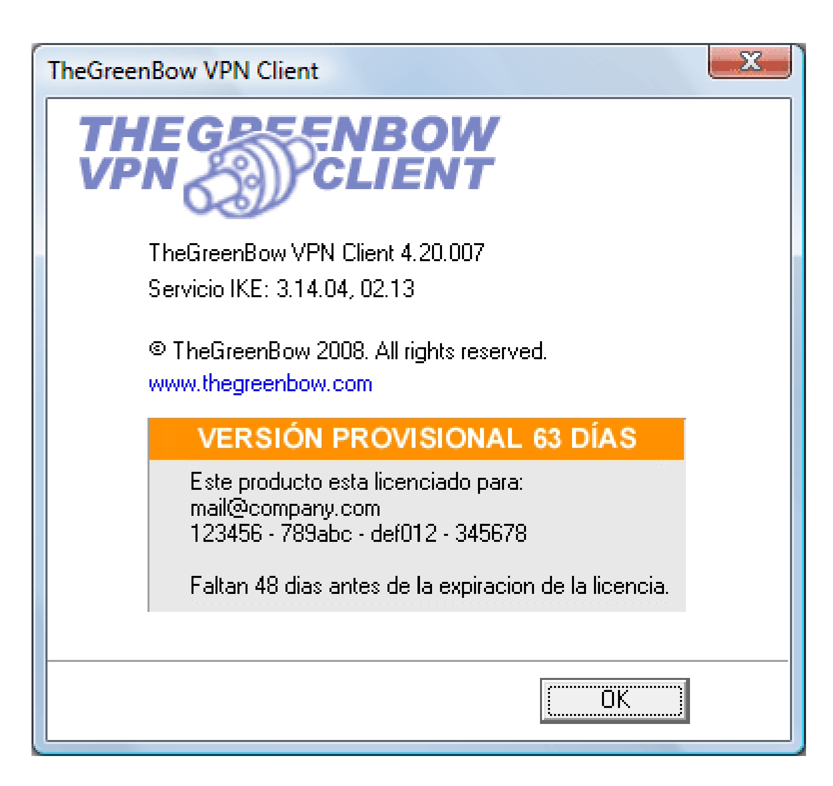
2.3 Licencia Temporal del Software

En períodos de prueba, podemos suministrar un Número de Licencia Temporal de Software. La validez de este período será de entre 1 y 35 semanas. Si quiere recibir un Número de Licencia Temporal del Programa, puede contactar nuestro departamento de ventas: sales@thegreenbow.es.

El período de validez del Número de Licencia Temporal de software y el tiempo de utilización restante aparecerán en la primera ventana automática del Cliente VPN IPSec. Cuando finalice el período de validez, no podrá ejecutar el software.



Durante todo el tiempo que esté usando un Número de Licencia Temporal del Software, puede acceder a la ventana de activación desde el Panel de Configuración para activar una nueva licencia, como por ejemplo, el Número de Licencia definitiva en lugar de una temporal.
Durante este período, puede visualizar el tiempo restante de la licencia a través del menú 'Acerca de', como se muestra a continuación:



Cuando el Número de Licencia Temporal de Software expire, el botón 'Evaluar' no aparecerá disponible. El usuario puede Comprar y Activar la licencia definitiva del software.

2.4 Activación del Software

2.4.1 Asistente de Activación del Software

Para poder usar después del período de evaluación, el programa Cliente VPN IPSec TheGreenBow debe estar activado en su ordenador. Para usar el Número de Licencia en un nuevo equipo, tendrá que desinstalar el software en el ordenador anterior, la desactivación se llevará a cabo automáticamente. La Activación del Software es un proceso de dos pasos que requiere el Número de Licencia y una dirección de correo electrónico.

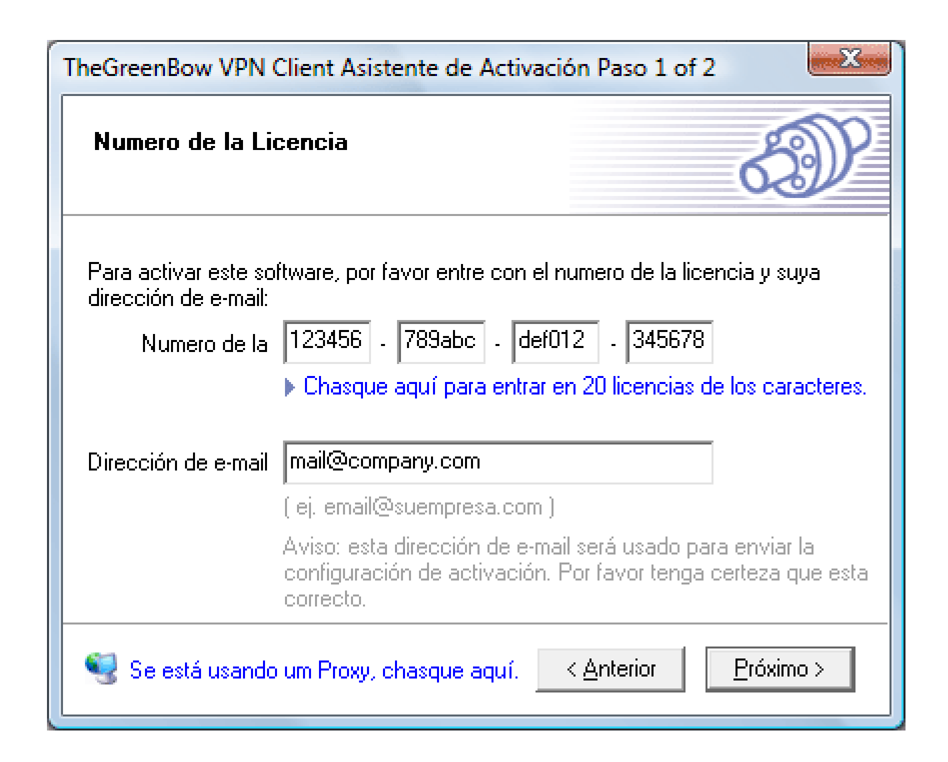
Puede iniciar el 'Asistente de Activación' de las siguientes maneras:

- Haciendo clic en el botón 'Activar' de la ventana de inicio cuando ejecuta el Cliente VPN.
- Haciendo clic en el menú '?' y después en "Asistente de Activación…".

2.4.2 Paso 1 de 2: Introducir el Número de Licencia

La activación del Software necesita un Número de Licencia.

Introduzca su Número Licencia, su dirección e-mail y seleccione 'Siguiente' como aparece indicado:



Atención: si dispone de un Número de Licencia de 20 caracteres, seleccione la opción para un Número de Licencia de 20 caracteres seleccionando en "Haga clic aquí para introducir una Licencia de 20 caracteres".

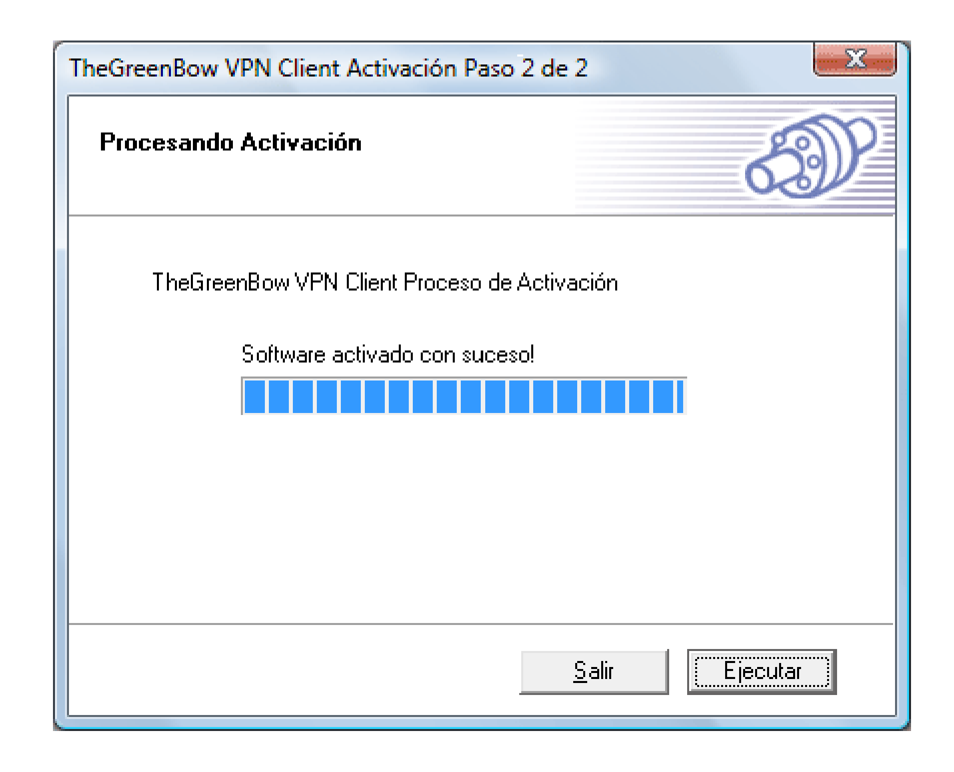
Nota: Asegúrese de que la dirección de correo electrónico es correcta, porque le confirmaremos por e-mail la activación.

Nota: Puede que no sea necesaria la dirección de correo electrónico: el Informático puede forzar este valor durante la instalación, que no aparecerá entonces en el Asistente de Activación del Software. Esta opción puede utilizarse para centralizar todos los correos de confirmación de Activación del Software en una única dirección de correo electrónico.

2.4.3 Paso 2 de 2: Activación Online

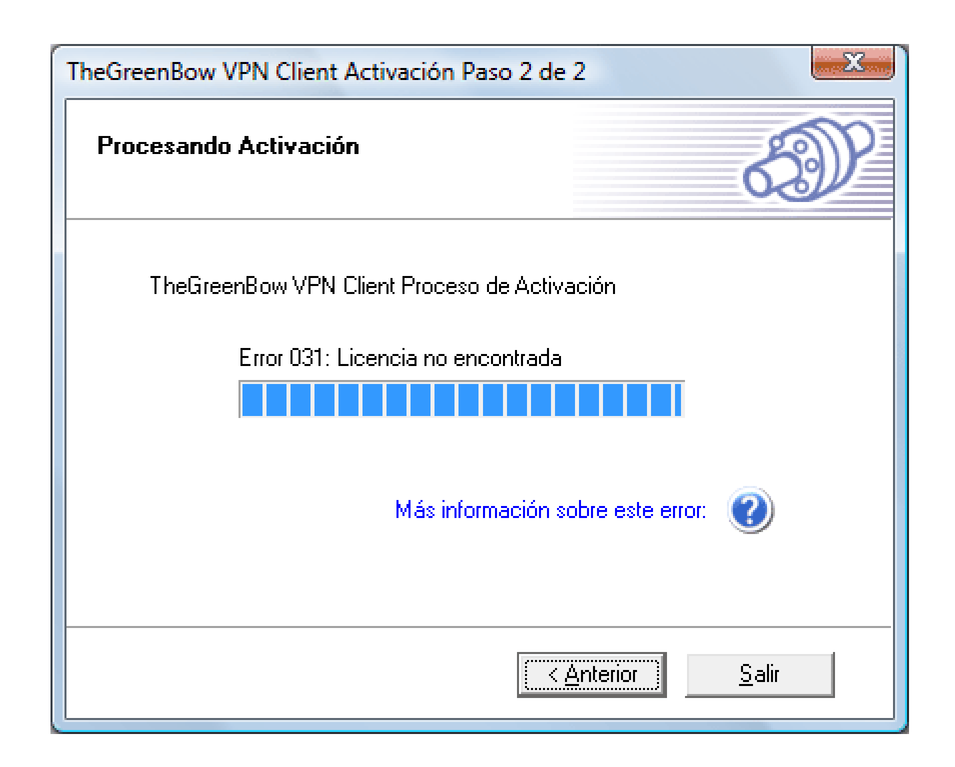
El 'Asistente de Activación' se conectará automáticamente al servidor de activación de software online para activar el Software del Cliente VPN. Puede volver atrás siempre que quiera para cambiar el Número de Licencia.

El 'Asistente de Activación' terminará tras haber realizado la Activación correctamente.



2.4.4 Problemas de Activación

Pueden ocurrir errores durante el proceso de activación. Cada error de activación está brevemente explicado en el paso 2 de la ventana de activación. Puede acceder online a todas las explicaciones y recomendaciones de cómo solucionar el problema haciendo clic en el campo "Más información acerca de este error", situado bajo la barra de progreso.



La mayoría de los errores se resuelvan verificando los siguientes puntos:

1. Compruebe que introdujo el Número de Licencia correcto (error 031).
2. La comunicación con nuestro servidor online de activación puede estar filtrada por un proxy (error 053 or error 054). Puede configurar el Proxy en el paso 1 del Asistente de Activación del Sofware haciendo clic en el botón correspondiente de la ventana.
3. La comunicación con nuestro servidor online de activación puede estar filtrada por un firewall (error 053 or error 054). Compruebe si un firewall personal o de la empresa está filtrando las comunicaciones.
4. Nuestro servidor de activación puede estar inaccesible temporalmente. Intente activar el software tras varios minutos.
5. Su Número de Licencia ya está activado (error 033). Contacte con nuestro departamento de ventas: sales@thegreenbow.es.

Todos los errores de activación se encuentran detallados en nuestra web: www.thegreenbow.com/help.html?subject=osa&id=001

Nota: Si no consigue activar el software satisfactoriamente a pesar de las recomendaciones anteriores, siempre podrá activarlo manualmente desde nuestra página web: www.thegreenbow.com/activation/osa_manual.html. Esta opción permite a los usuarios efectuar una activación completa e inmediata del software.

2.5 Actualización del Software

Atención: Tiene que activar el software del Cliente VPN después después de cada actualización del software.
Se tarda unos cuantos segundos. En función de su contrato de mantenimiento, la activación de la actualización del software puede verse rechazada. Por favor, lea atentamente las siguientes recomendaciones y compruebe el estado actual de su contrato de mantenimiento, haciendo clic en el menú "?", después en "Buscar actualizaciones" en el Panel de Configuración.

El éxito de la activación del software actualizado dependerá de su contrato de mantenimiento:

1. Todas las activaciones del software están permitidas durante su período de mantenimiento (que empieza con la primera activación).
2. Cuando expire el período de activación (o si carece de contrato de mantenimiento), sólo podrá realizar actualizaciones de versiones de mantenimiento. Puede identificar las actualizaciones de las versiones de mantenimiento por el último dígito de la versión.

Ejemplo: Mi período de mantenimiento expiró y mi actual versión del programa es 3.12. Sólo podrá actualizar desde las versiones 3.13 a la 3.19. No puede actualizar las versiones 3.20, 3.30 o 4.00.

Si desea suscribirse al contrato de mantenimiento o ampliarlo, por favor contacte con nuestro departamento de ventas: sales@thegreenbow.es

Nota: La Configuración VPN se guardará durante la Actualización del Software y automáticamente aparecerá disponible con la nueva versión.

2.6 Desinstalación del Software

Cliente VPN IPSec TheGreenBow puede desinstalarse:

- desde el Panel de Control de Windows seleccionando 'Agregar o quitar programas'
- desde el Menú Inicio > Programas > TheGreenBow > VPN > 'Desinstalar Cliente VPN IPSec'



Consejos Prácticos

3 Consejos Prácticos

3.1 Cómo Abrir un túnel VPN?

Cómo abrir un túnel VPN (una vez configurado):
- Panel de conexión > Abrir
- Icono en la barra de tareas > clic en 'Abrir xxx'
- 'Automático al detectar el tráfico'
- 'Automático al detectar una memoria USB'
- 'Automático al iniciar MS Windows' (antes o después de conectarse)
- Haciendo doble clic en una Configuración VPN (en un icono del escritorio o en un archivo adjunto del correo electrónico, por ejemplo)
- Líneas de comando permite abrir o cerrar los túneles

3.2 Cómo Verificar un túnel VPN?

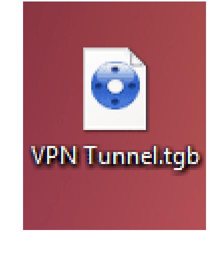
Para poder solucionar los errores de un túnel VPN, puede recurrir a los siguientes documentos disponibles en nuestro sitio web:
- TroubleShooting Document (pdf).
- Ayuda online (html).
- Ayuda online para la Activación del Software (html).
- Utilice la Configuración VPN por defecto para verificar su conexión de red.
- Ver también las Preguntas Frecuentes acerca del Cliente VPN IPSec.

3.3 Cómo importar una Configuración VPN con un simple doble clic?

También conocido como 'modo Dial up', puede abrir un túnel mediante un doble clic en una Configuración VPN (extensión archivo '.tgb'). Esta opción permite crear varias Configuraciones VPN en el escritorio, y abrir túneles haciendo clic en el icono de acceso directo de cada una de ellas.

Cómo crear un icono de acceso directo de una Configuración VPN en el escritorio:
Paso 1: Configura el túnel en el 'Panel de Configuración'
Paso 2: En 'Parámetros Avanzados de la Fase 2', configura el túnel en "Abrir automáticamente este túnel cuando se inicie el Cliente VPN'
Paso 3: Exporte la Configuración VPN al escritorio del ordenador.

Nota: Puede proteger la Configuración VPN con contraseña al exportarla. Se le pedirá la contraseña cada vez que haga clic en el icono.



Parte



Navegar en la Interfaz de Usuario

4 Navegar en la Interfaz de Usuario

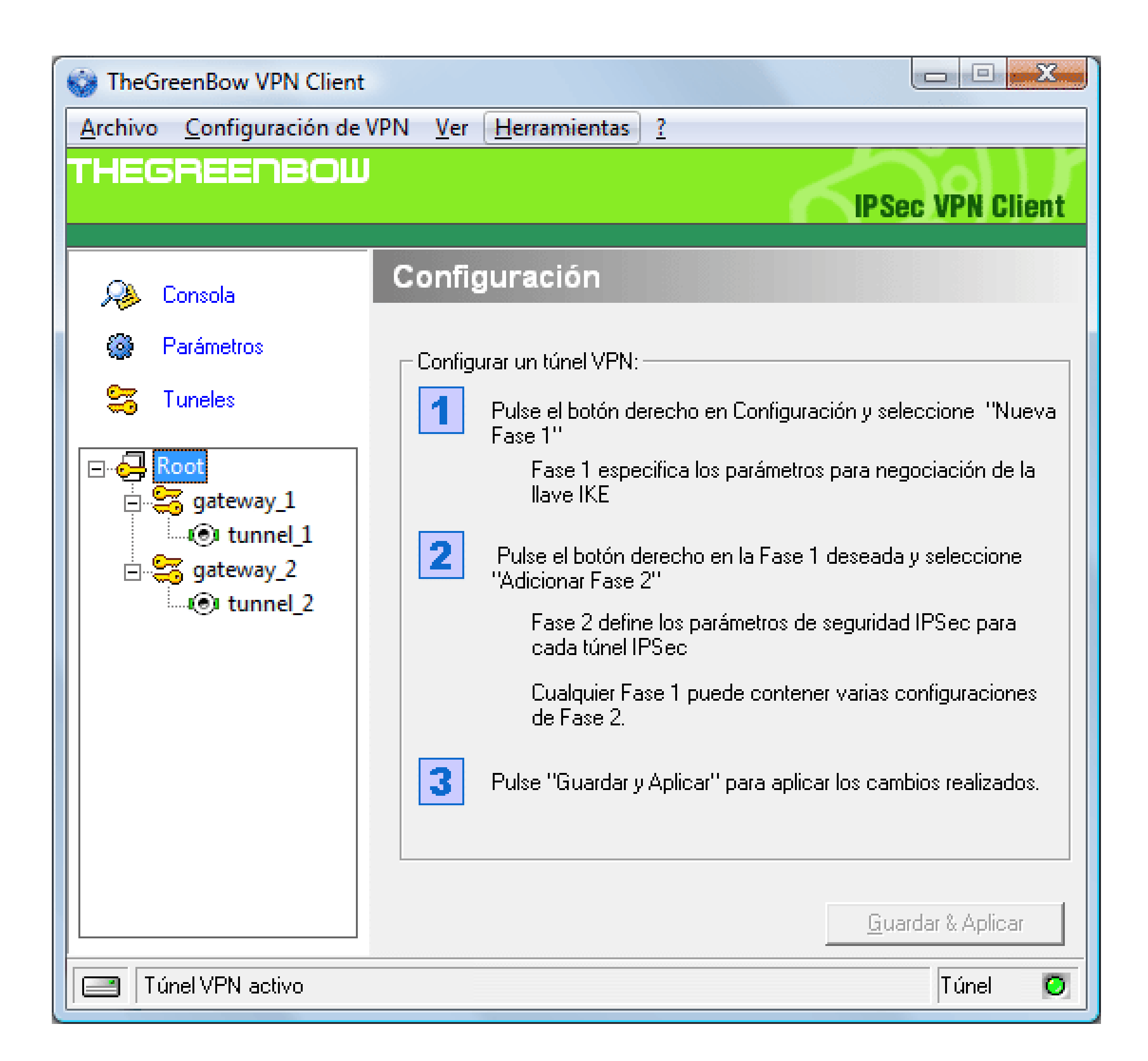
4.1 Interfaz de usuario

El Cliente VPN IPSec TheGreenBow es totalmente autónomo y puede abrir y cerrar túneles sin la intervención del usuario, en función del tráfico hacia determinadas direcciones. Con todo, necesita ser configurado.

La configuración del Cliente VPN IPSec está definida en un archivo de configuración VPN. La interfaz del programa permite crear, modificar, guardar, exportar e importar configuraciones VPN junto con elementos de seguridad (como Claves Partilhadas, Certificados,...).

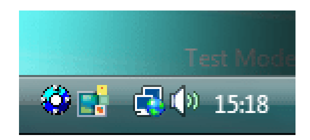
La interfaz de usuario está compuesta por diferentes elementos:

- Panel de Configuración
- Panel de Conexión
- Menús Principales
- Icono en la Barra de Herramientas & Popup
- Asistentes
- Wizards
- Preferencias



4.2 Icono de la Barra de Herramientas

La interfaz de usuario del Cliente VPN puede iniciarse haciendo un doble clic en el icono de la aplicación (en el escritorio o en el menú de inicio) o un simple clic en el icono en la barra de herramientas. Cuando ya está abierto, el Cliente VPN muestra un icono en la barra de herramientas que indica el estado de los túneles con un color:

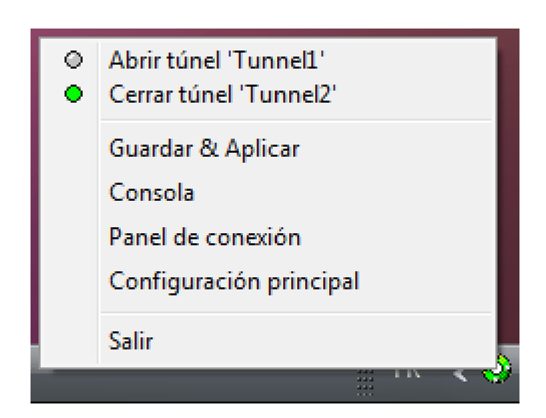


El código de colores es el que aparece a continuación:

 Icono azul: no hay ningún túnel VPN abierto.

 Icono verde: al menos un túnel VPN está abierto.

Un clic con el botón izquierdo del ratón sobre el icono VPN abrirá la configuración de la interfaz de usuario.



Un clic con el botón derecho desplegará el siguiente menú:
- 'Salir' cierra los túneles VPN establecidos y detiene la configuración de la interfaz de usuario.
- 'Guardar y Aplicar' cierra los túneles VPN establecidos, aplica la última modificación de la configuración y vuelve a abrir todos los túneles VPN.
- 'Consola' muestra la ventana de registros.
- 'Panel de Conexión' abre la lista de los túneles VPN que están establecidos. Puede configurar que los túneles se abran automáticamente al iniciar el programa.
- Lista de túneles configurados con su estado actual. Los túneles también se pueden abrir o cerrar desde este menú.

Mensajes emergentes del icono del Cliente VPN mostrará el estado de la conexión del túnel VPN:
- 'Túnel <nombredeltúnel>' cuando se establecen uno o más túneles
- 'Espere VPN listo…' cuando el servicio IKE se reinicia
- 'Cliente VPN TheGreenBow' cuando el Cliente VPN está funcionando sin ningún túnel abierto.

4.3 System Tray Popup

Un pequeño popup systray aparece cada vez que un túnel se abra o se fecha.

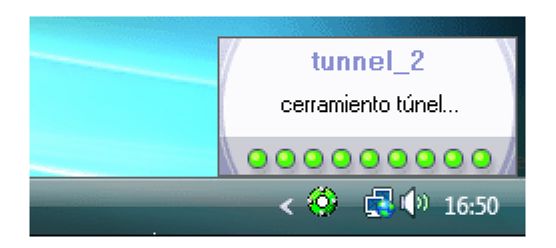
Este pequeño popup tiene un comportamiento muy simple:

1. El popup muestra la apertura de túnel con diferentes fases e desaparece después de 6 segundos a menos que el ratón se mueve sobre.





1. El popup muestra también el cerramiento del túnel.





2. En caso de que el túnel no puede abrir, se mostrará una advertencia con un enlace a más información en nuestra pagina web.



4.4 Accesos Directos del Teclado

Esta opción facilita el acceso a las funciones más frecuentes del programa.

Acceso Directo	**Acción**
Ctrl + Enter	Alterna de ida y vuelta entre el 'Panel de Configuración' and the 'Panel de Conexión'. Nota: si el Panel de Configuración está protegido con contraseña, se le preguntará al usuario por la contraseña cuando intente cambiar al Panel de Configuración.
Ctrl + D	Abre la 'Consola' VPN para 'Debug' de conexión.
Ctrl + S	‘Guardar y Aplicar’ una Configuración VPN

4.5 Panel de Conexión

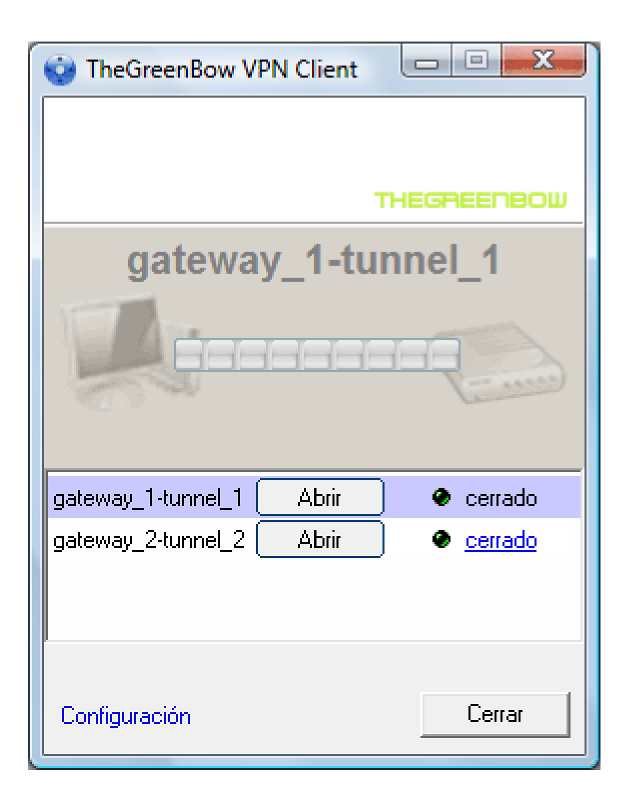
El Panel de Conexión permite a los usuarios abrir, cerrar y obtener una información clara sobre cada uno de los túneles que se han configurado. Esto es todo las necesidades que precisa el usuario final para abrir y cerrar los túneles.
Esta característica ayuda claramente ambos administradores (que configuran las conexiones VPN) y los usuarios (que sólo abran o cerran conexiones VPN) con su propio uso.

El panel de conexión está hecha de varios elementos:

- Un diagrama animado de red que muestra la información sobre el túnel (arriba)
- Una lista de todos los túneles configurado con un botón 'abrir / cerrar' (diagrama abajo)

- Un enlace de vuelta al 'Panel de Configuración "(parte inferior izquierda)

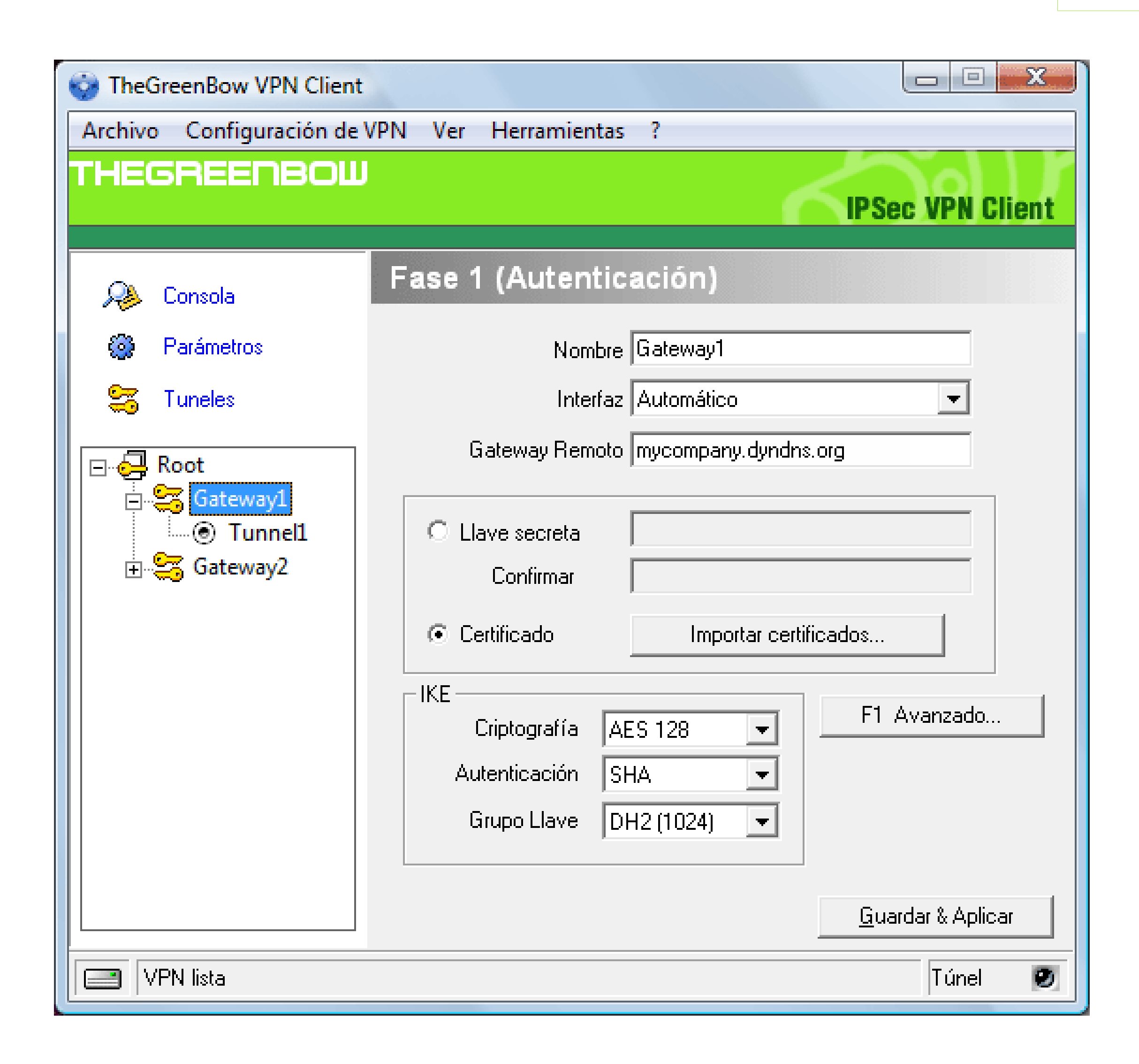
Es posible cambiar de ida y vuelta entre el 'Panel de Conexión' y el 'Panel de Configuración utilizando el atajo 'Ctrl + Enter' (ver sección 'Atajos').



4.6 Panel de Configuración

El Panel de Configuración está compuesto por diferentes elementos:

- Tres botones: 'Consola', 'Parámetros' y 'Túneles' (columna de la izquierda)
- Una ventana con una lista en árbol que contiene las configuraciones IKE e IPSec (columna de la izquierda)
- Una ventana de configuración vinculada con el nivel elegido del árbol (columna de la derecha)



Puede arrastrar y soltar un archivo de Configuración VPN (extensión '.tgb') en el Panel de Configuración. Esta opción permite aplicar una nueva configuración VPN de una manera más fácil. Si un túnel está configurado para "abrirse cuando se inicie el Cliente VPN' (ver apartado ' Fase 2 Opciones Avanzadas'), se abrirá inmediatamente tan pronto como se aplique la nueva Configuración VPN ('Guardar y Aplicar').

4.6.1 Menús Principales

Entre los muchos menús que posee, puede encontrar:

- El menú '**Archivo**' se utiliza para Importar o Exportar una configuración o para elegir la localización de la Configuración VPN: local, USB, servidor o Token. También puede configurar las preferencias así como el modo de inicio del Cliente VPN (antes o después de conectarse,etc).
- El menú '**Configuración VPN**' contiene todas las acciones desde el menú contextual del botón derecho. El menú 'Configuración' también permite acceder a la 'Configuración del Asistente'.
- El menú **'Ver'** permite configurar los elementos a los que puede acceder el usuario. El menú '**Herramientas**' contiene las opciones 'Consola', 'Conexiones' y 'reset IKE'.
- El menú **'?'** permite acceder a 'Verificar actualizaciones', 'Ayuda Online' y a la ventana 'Sobre...'. También permite acceder a la 'Configuración del Asistente'.

4.6.2 Barra de Estado

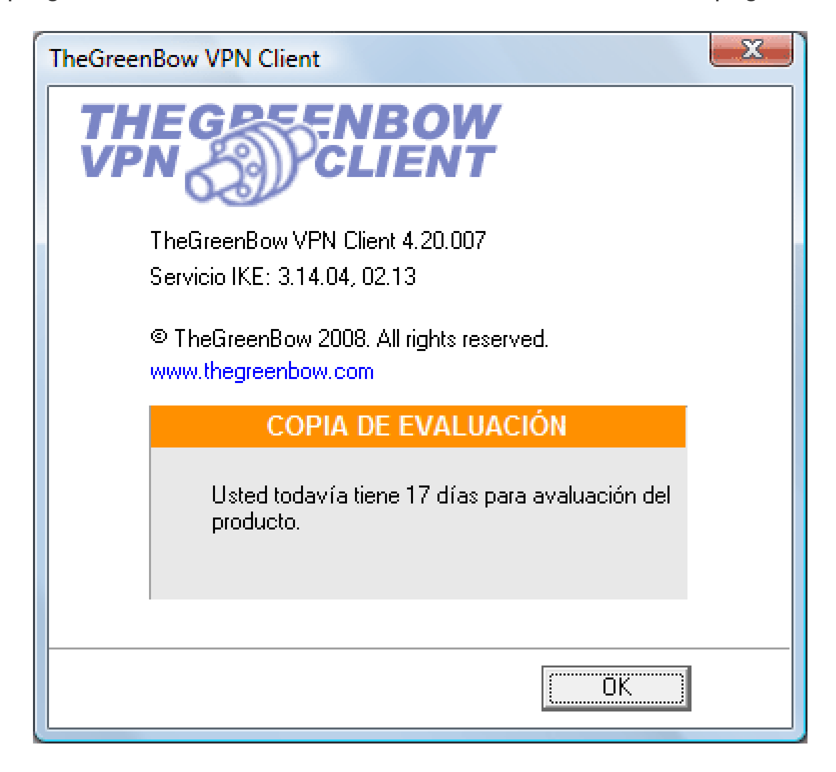
La barra de estado ofrece informaciones varias:



- La zona izquierda indica la localización de la configuración VPN. Por ejemplo, si está en funcionamiento el 'Modo USB', la imagen mostrará una memoria USB, que estará disponible sólo si se detecta una memoria USB de VPN válida.
- La zona central proporciona información acerca del estado del programa Cliente VPN ("abriendo túnel", "guardando las opciones de configuración" o "iniciando el Cliente VPN", entre otros).
- La luz en el lado derecho informa acerca de los túneles (por ejemplo, Luz verde Túnel significa que al menos un túnel está abierto, Luz Gris Túnel significa que ningún túnel está abierto)

4.6.3 Ventana 'Sobre...'

La ventana 'Sobre...' indica la versión del software del Cliente VPN e información sobre la activación del programa. También encontrará un acceso directo a nuestra página web.

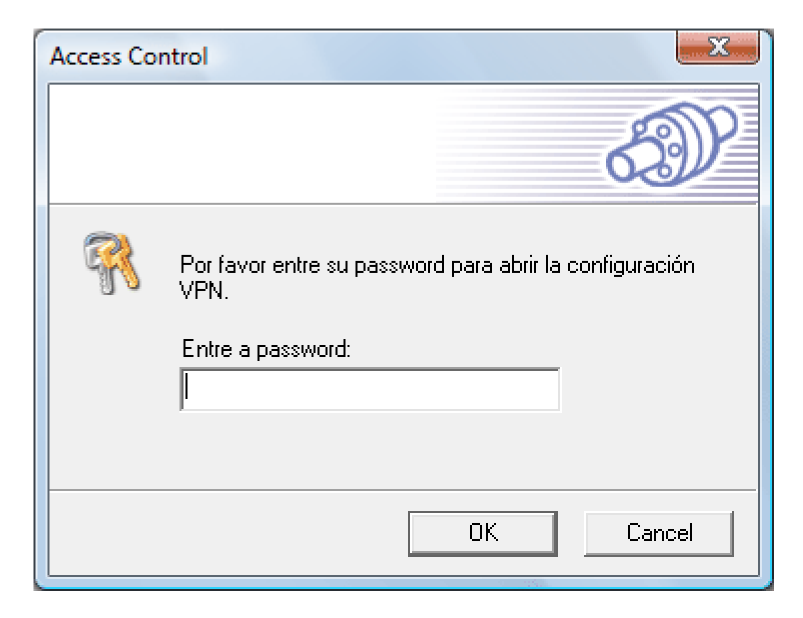


4.6.4 Control de Acceso e Interfaz Oculta

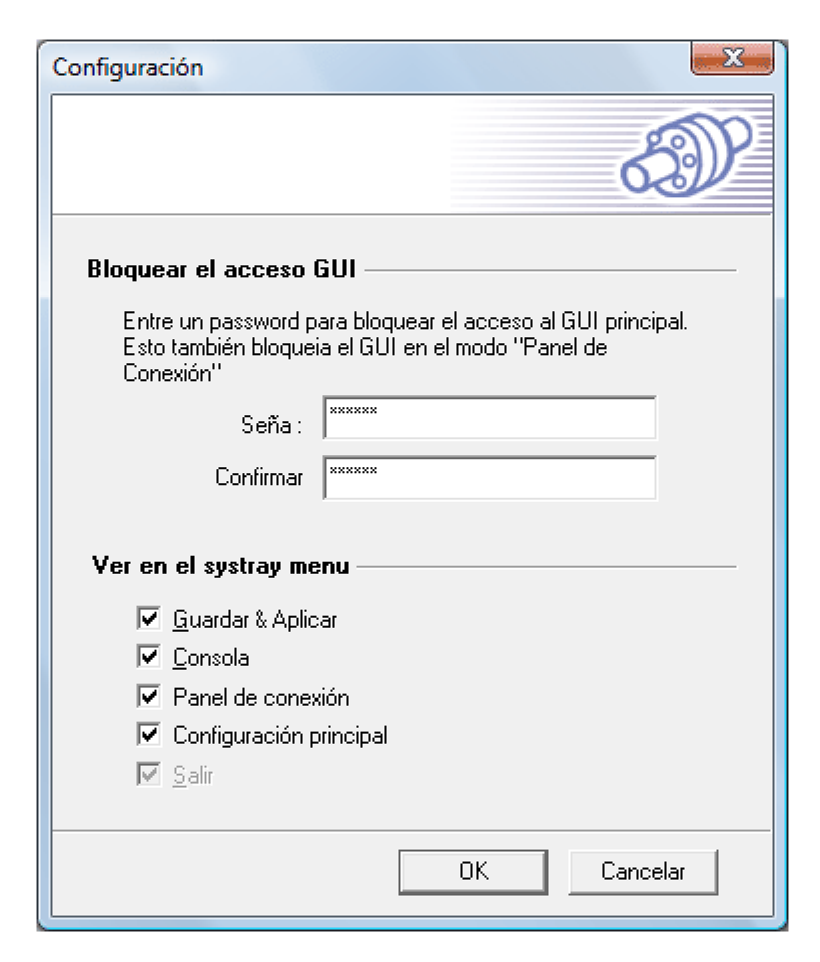
Esta función está especialmente diseñada para los Administradores. Permite bloquear el acceso al Panel de Configuración y restringir con contraseña el acceso del usuario del Cliente VPN IPSec al 'Panel de Conexión' y/o al menú de la barra de tareas. De este modo, los usuarios no pueden modificar la Configuración VPN, evitando así configuraciones defectuosas.

Una vez configurado, le pedirá la contraseña al usuario:

1. cuando haga clic o doble clic en el icono del Cliente VPN IPSec en la bandeja del sistema
2. cuando cambie del ‘Panel de Conexión’ al ‘Panel de Configuración’.



Esta contraseña puede configurarse como opción en la instalación (ver apartado ‘opciones de instalación’).
La ventana de Control de acceso está disponible a través del menú ‘Ver' > 'Configuración’ en el Panel de Configuración, que también permite configurar los elementos del menú de la bandeja del sistema. Así, el Informático puede restringir el acceso al programa, desde el acceso total a la interfaz oculta.

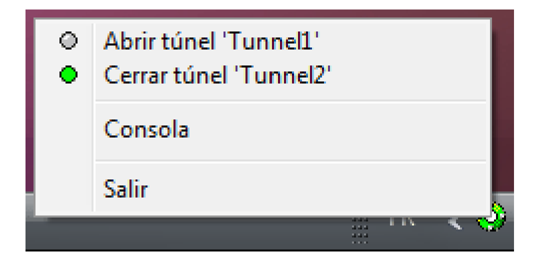


Para modificar el control de acceso, sólo rellene los campos 'Contraseña' y 'Confirmar' y luego haga clic en 'Aceptar'.

Nota: El campo 'Salir' del menú de la bandeja del sistema está deshabilitado en la versión estándar del programa. No obstante puede modificarse durante la instalación del mismo, a través de la la opción de instalación "-menuitem" (véa la sección 'Opciones de Instalación')

El control de acceso con contraseña sólo afecta al 'Panel de Configuración'. Nunca se podrá controlar el acceso al 'Panel de Conexión' con contraseña.

Si el Control de Acceso se ha activado, el 'Panel de Configuración' no podrá abrirse ni verse haciendo doble clic en el icono del escritorio o seleccionándolo en el menú de Inicio. Con un clic derecho sobre el icono en la barra de tareas sólo podrá acceder a 'Consola', saliendo del programa y abriendo o cerrando los túneles configurados:



4.6.5 Asistentes

Existen dos Asistentes disponibles:

- El Asistente de Configuración VPN, que puede iniciarse desde el Menú 'Configuración VPN' > 'Asistente de Configuración'.

- El Asistente de Activación del Software, que puede iniciarse desde el Menú '?' > 'Asistente de Activación'.

4.6.6 Preferencias

La ventana 'Preferencias' le permite definir:

- El modo de inicio del programa. Puede configurar los diferentes modos durante la instalación (ver apartado 'Opciones de Instalación').
- Habilitar/Deshabilitar la detección de desconexión de la interfaz de red

Puede acceder a las preferencias a través del Menú 'Archivo' y haciendo clic en 'Preferencias'.



Modo de inicio del Cliente VPN
El Cliente VPN IPSec TheGreenBow dispone de diferentes modos de inicio, entre ellos:

- 'Iniciar el Cliente VPN IPSec antes del inicio de sesión en Windows': este modo puede utilizarse para securizar un inicio de sesión remoto.
- 'Iniciar el Cliente VPN IPSec tras el inicio de sesión en Windows'
- 'No iniciar el Cliente VPN IPSec cuando inicie el Windows': el Cliente VPN IPSec se inicia manualmente por el usuario (modo "manual")

Diversos
Deshabilitar la detección de la desconexión de la interfaz permite que el Cliente VPN IPSec mantenga los túneles abiertos mientras la interfaz de red se desconecta momentáneamente pero con frecuencia. Esto ocurre cuando la interfaz que se utiliza para abrir túneles es inestable, como una WiFi, GPRS y todas las interfaces 3G.

Parte



Panel de Conexión

5 Panel de Conexión

5.1 Bases del Panel de Conexión

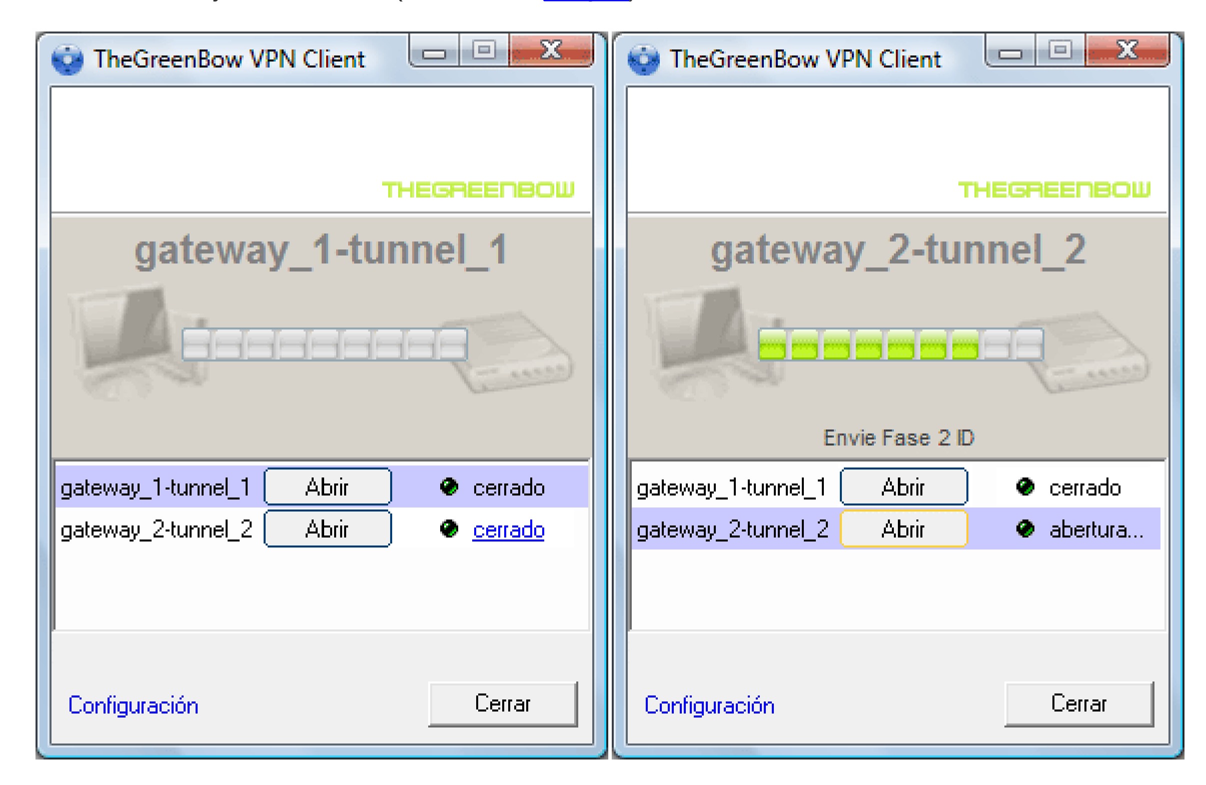
El Panel de Conexión permite abrir, cerrar y obtener información clara acerca de cada uno de los túneles que han sido configurados. Esto es todo lo que el usuario necesita para abrir y cerrar túneles. Es evidente que esta opción ayuda tanto el Administrador (que configura las conexiones VPN) como a los usuarios (que sólo abren y cierran conexiones VPN).

El Panel de Conexión está compuesto por diferentes elementos:

- Un diagrama de red animado que muestra información sobre el túnel en uso (arriba)
- Una lista de todos los túneles configurados con el botón 'abrir/cerrar' (bajo el diagrama)

Para abrir un túnel, el usuario simplemente tiene que hacer clic en el botón 'Abrir' del túnel. El botón 'Abrir' cambiará automáticamente a 'Cerrar' cuando se abra un túnel. Un clic sobre el nombre del túnel abrirá automáticamente el Panel de Configuración, que permite modificar la configuración del túnel. Esta opción aparece deshabilitada cuando el Panel de Conexión está protegido por contraseña (ver apartado 'Control de Acceso').

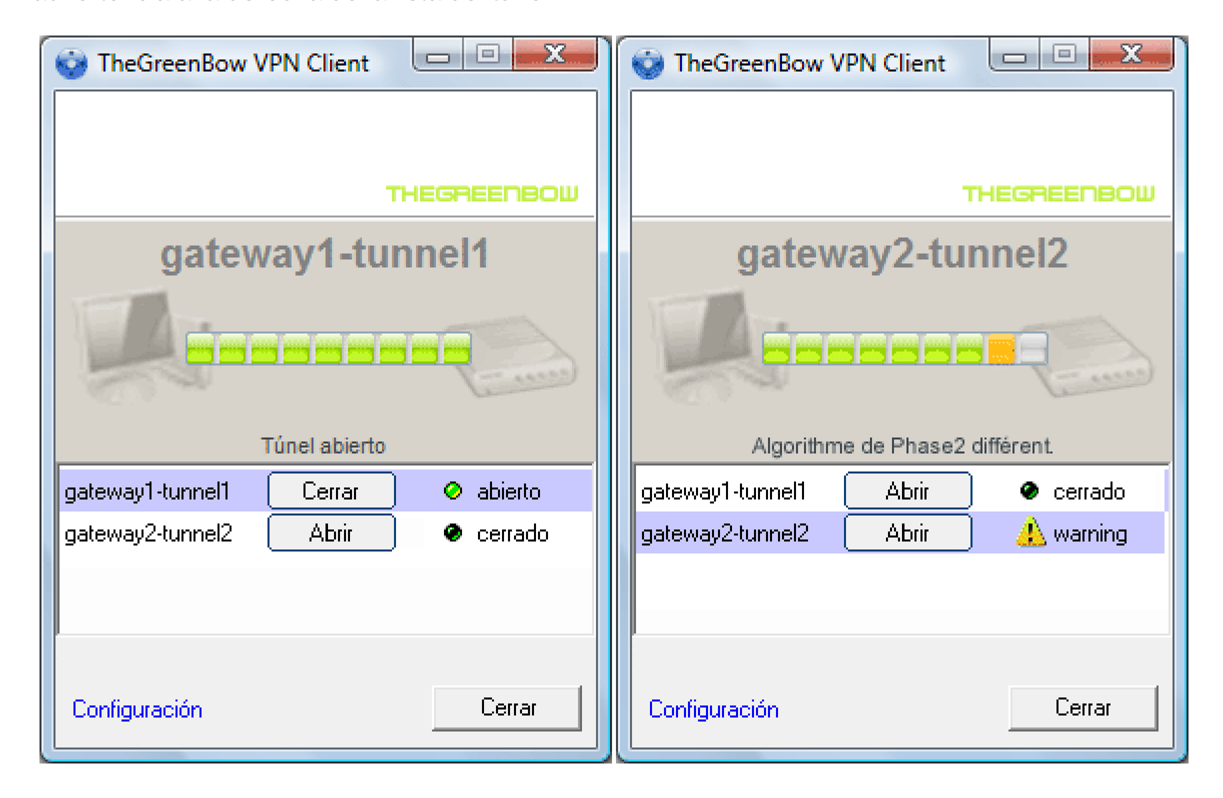
Es posible cambiar de ida y vuelta entre el 'Panel de Conexión' y el 'Panel de Configuración' utilizando el atajo 'Ctrl + Enter' (ver sección 'Atajos').



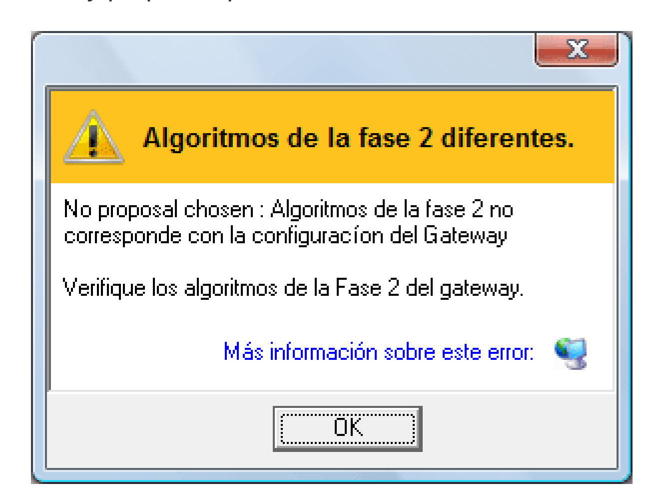
También es posible aplicar automáticamente una nueva Configuración VPN arrastrando y soltando una Configuración VPN en el Panel de Conexión. Si un túnel está configurado para "abrirse cuando se inicie el Cliente VPN" (ver apartado 'Fase 2 Opciones Avanzadas'), se abrirá inmediatamente tan pronto como se aplique la nueva Configuración VPN ('Guardar y Aplicar').

5.2 Más Información de Conexión

Cuando se produce un problema durante el proceso de apertura del túnel, aparecerá una advertencia a la derecha de la lista del túnel.



Haciendo clic en la advertencia abrirá automáticamente una ventana que le mostrará el problema de manera detallada. Los mensajes explícitos de advertencia ayudan a identificar el problema, tanto a los usuarios como a los Informáticos. Estos mensajes instantáneos también le ponen en contacto con nuestras páginas web de ayuda online (seleccionando "más información"), que detallan los síntomas de errores y proponen posibles soluciones.





Configuración VPN

6 Configuración VPN

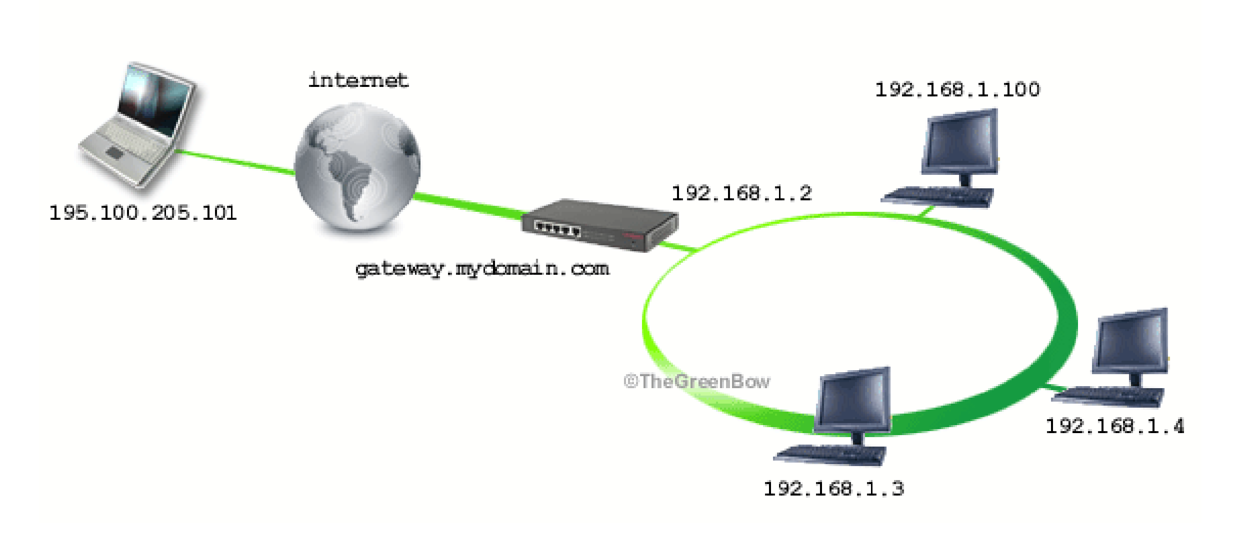
6.1 Asistente de Configuración

6.1.1 Asistente de Configuración en tres pasos

El Cliente VPN IPSec TheGreenBow dispone de un Asistente de Configuración que permite crear una configuración VPN en tres sencillos pasos. Este Asistente de Configuración está diseñado para ordenadores remotos que necesitan conectarse a la empresa LAN a través de una gateway VPN. Recuerde que el modo Peer to Peer también está disponible .

Observemos el siguiente ejemplo:

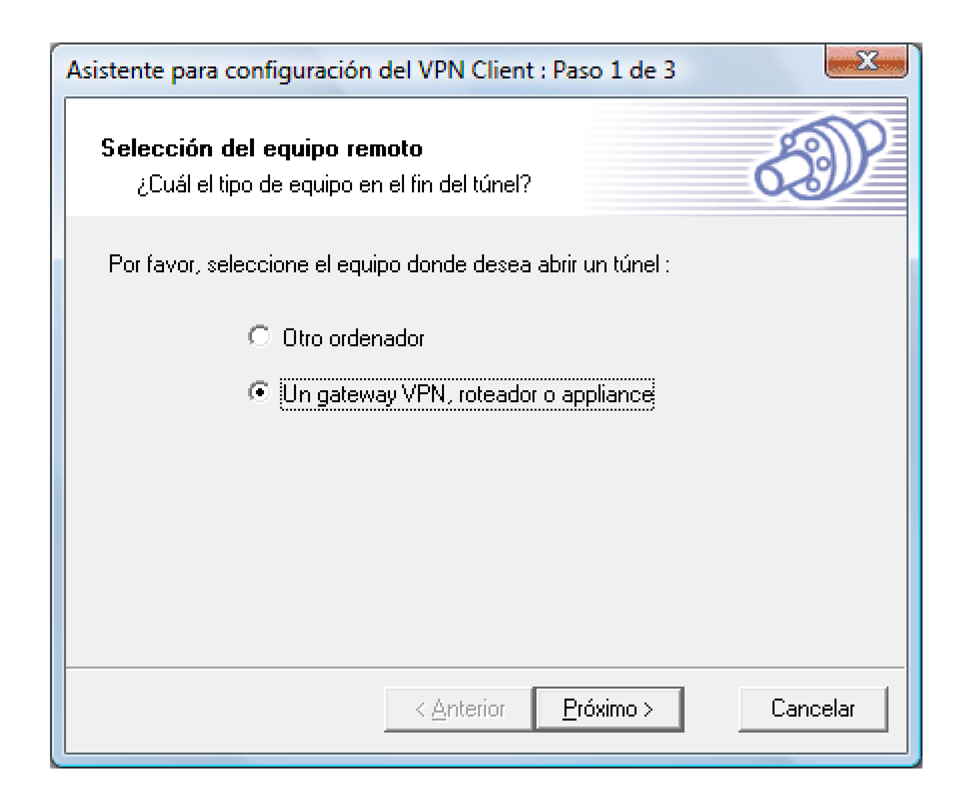
- El ordenador remoto posee una dirección IP pública dinámica.
- Intenta conectarse a la red LAN de la empresa a través de una gateway VPN que tiene la dirección DNS "gateway.mydomain.com".
- La dirección de la red LAN de la empresa es 192.168.1.xxx. Por ejemplo, el ordenador remoto quiere conectarse a un servidor con la dirección IP: 192.168.1.100.



Para configurar la conexión, abra la ventana del asistente seleccionando el menú "Configuración > Asistente".

6.1.2 Paso 1 de 3: Elegir el equipo remoto

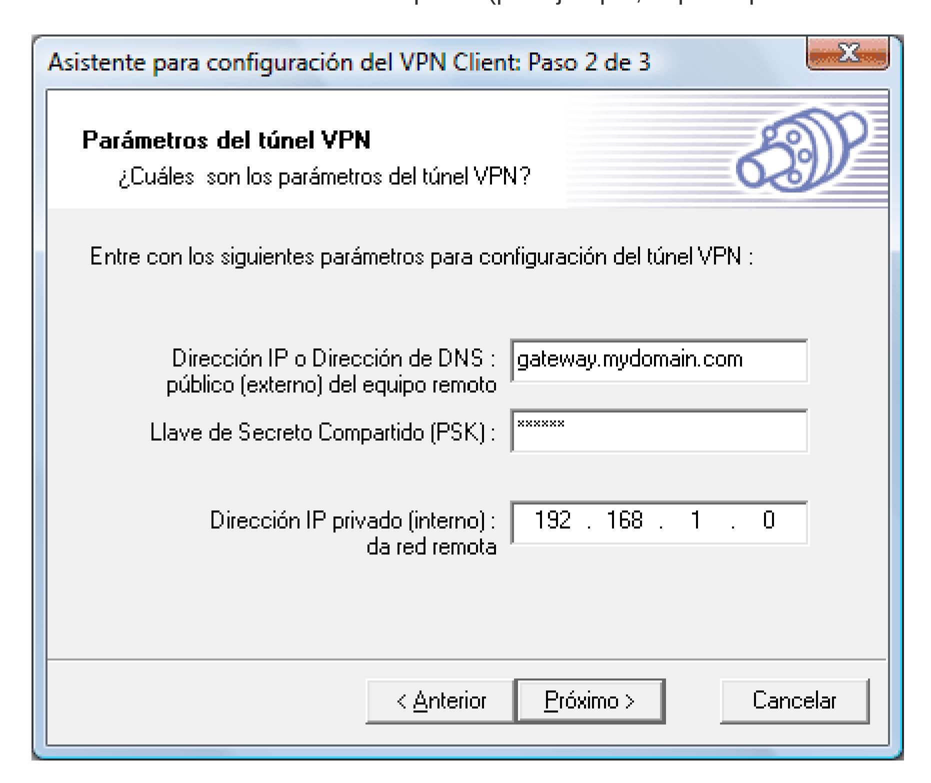
Debe especificar el tipo de equipo que se encuentra al final del túnel: Gateway VPN.



6.1.3 Paso 2 de 3: Parámetros del túnel VPN

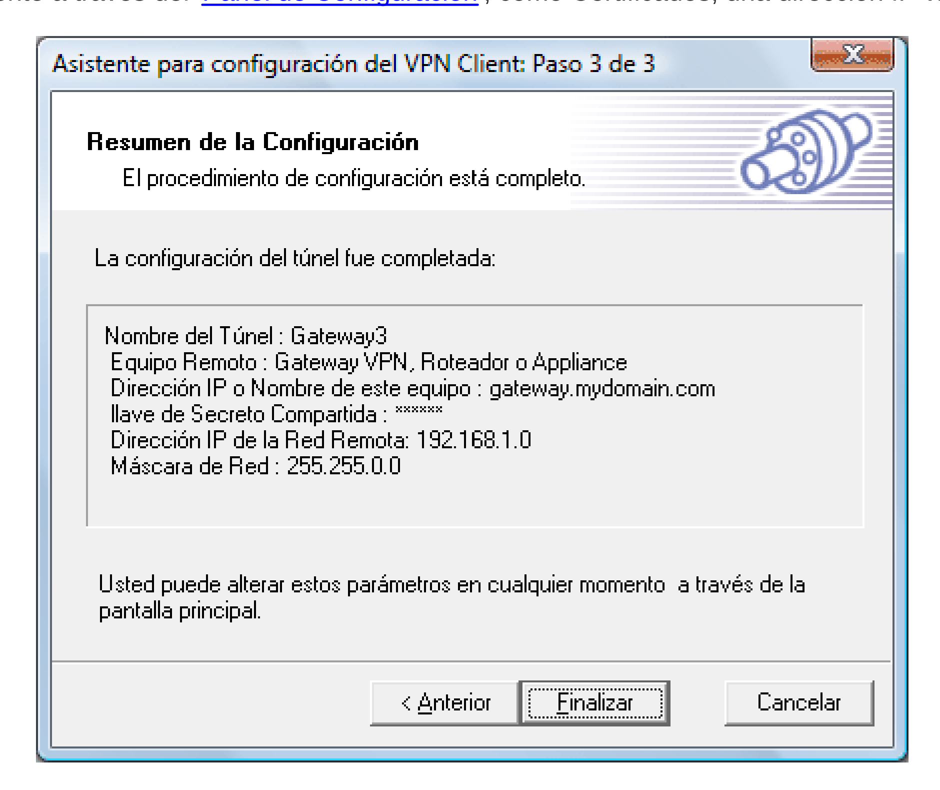
Es preciso que especifique la siguiente información:

- La dirección IP pública (parte del servidor Internet) de la gateway remota.
- la Clave compartida (PSK) que utilizará para este túnel (debe ser la misma que la de la gateway)
- la dirección IP de la red LAN de su empresa (por ejemplo, especifique 192.168.1.0)



6.1.4 Paso 3 de 3: Resumen

El tercer paso resume la nueva configuración VPN. Puede configurar otros parámetros directamente a través del 'Panel de Configuración', como Certificados, una dirección IP virtual, etc.

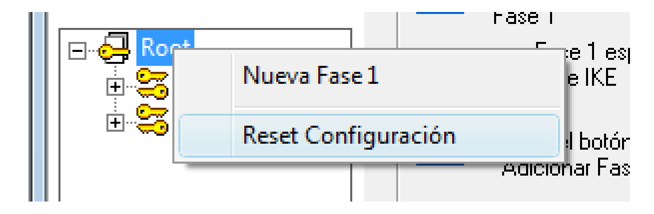


6.2 Configuración del Túnel VPN

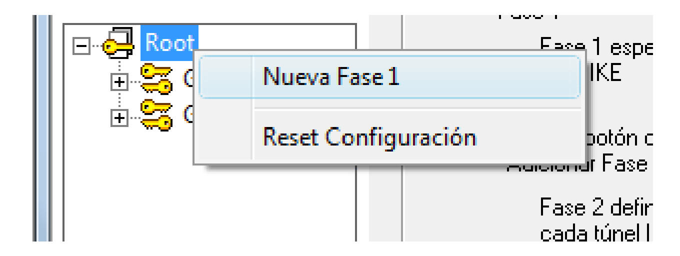
6.2.1 Cómo crear un túnel VPN?

Para crear un túnel VPN desde el Panel de Configuración (sin utilizar el Asistente de Configuración), debe seguir los siguientes pasos:

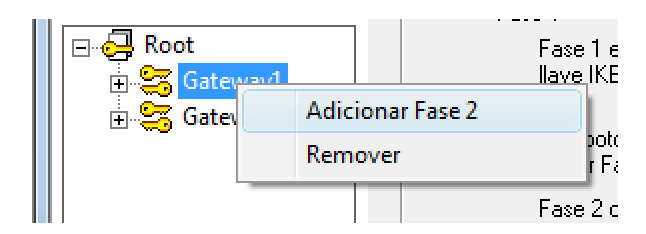
1. Reset el Panel de Configuración para eliminar cualquier configuración.



2. Haga clic derecho en 'Configuración' y seleccione 'Nueva Fase 1'.



3. Configura la Fase de Autenticación (Fase 1).
4. Haga clic derecho en la 'nueva Phase 1' y seleccione 'Añadir Fase 2'.



5. Configura la Fase IPSec (Fase 2).
6. Una vez que los parámetros estan configurados, haga clic en "Guardar y Aplicar 'para tener en cuenta la nueva configuración. De esta manera, el servicio IKE se ejecutará con los nuevos parámetros.
7. Haga clic en "Abrir túnel' para establecer el túnel VPN IPSec (sólo en la ventana " Configuración IPSec").

Por favor refiérase a la Fase 1 and Fase 2 para la descripción de las configuraciones.

6.2.2 Autentificación Múltiple o Fase de Configuración IPSec

Pueden configurarse varias Fases de Autentificación (Fase 1). Así, un ordenador puede establecer conexiones VPN IPSec con varias gateways o otros ordenadores (peer to peer).

Del mismo modo, pueden crearse varias Configuraciones IPSec (Fase 2) para una misma Fase de Autentificación (Fase 1).

6.2.3 Opciones Avanzadas

Para las Fases 1 y 2 puede definir opciones y parámetros avanzados.

Aquellos parámetros definidos en la Fase 1 se aplicarán a todos los de la Fase 2 creados en la Configuración VPN en uso:

- Habilitar/Deshabilitar el Modo Configuración
- Habilitar/Deshabilitar el Modo Agresivo NAT-T
- Habilitar/Deshabilitar la Gateway Redundante
- Seleccionar el modo NAT-T (Forzado, Deshabilitado o Automático)
- Establecer el registro X-Auth o la contraseña con la opción de mensajes emergentes

Aquellos parámetros definidos en la Fase 2 sólo se aplicarán a los de las Fases 2:

- Modo de Apertura Automática
- Elegir que arranque el Script/Aplicación cuando se abra el túnel
- Parámetros manuales de las direcciones del servidor DNS/WINS

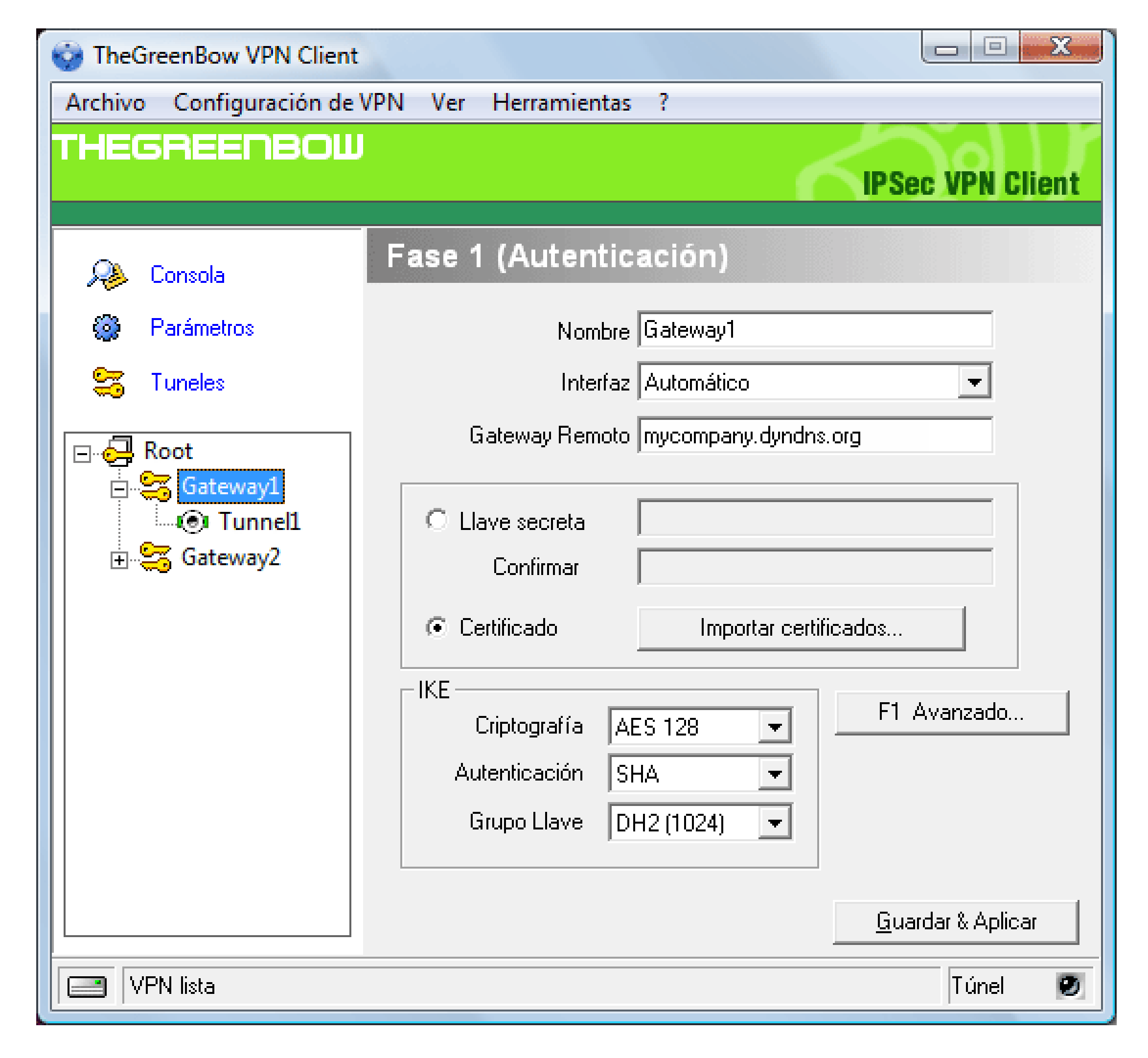
6.3 Autentificación o Fase 1

6.3.1 Qué es la Fase 1?

La ventana ‘Autentificación’ o ‘Fase 1’ concierne a los parámetros para la Fase de Autentificación o Fase 1, lo que también se conoce como Fase de Negociación IKE.

El objetivo de la Fase 1 es negociar los parámetros de seguridad IKE, verificar la autentificación de los usuarios y establecer un canal seguro entre los usuarios. Como parte de la Fase 1, cada sistema final debe identificarse y autentificarse al otro sistema.

6.3.2 Descripción de los Parámetros de la Fase 1



Nombre La etiqueta para la fase de Autentificación sólo se emplea en la configuración de la interfaz de usuario. Este valor nunca se utilizará durante la negociación IKE. Es posible cambiar el nombre en cualquier momento y leerlo en la estructura en árbol. Dos Fases 1 no pueden tener el mismo nombre.

Interfaz Dirección IP de la interfaz de red del ordenador, a través se establezca la conexión VPN. Si la dirección IP puede cambiar (cuando se recibió dinámica de un ISP), seleccione "Automático".

Gateway Remoto Dirección IP o dirección DNS de la gateway remota (en nuestro ejemplo: mycompany.dyndns.org). Este campo es obligatorio.

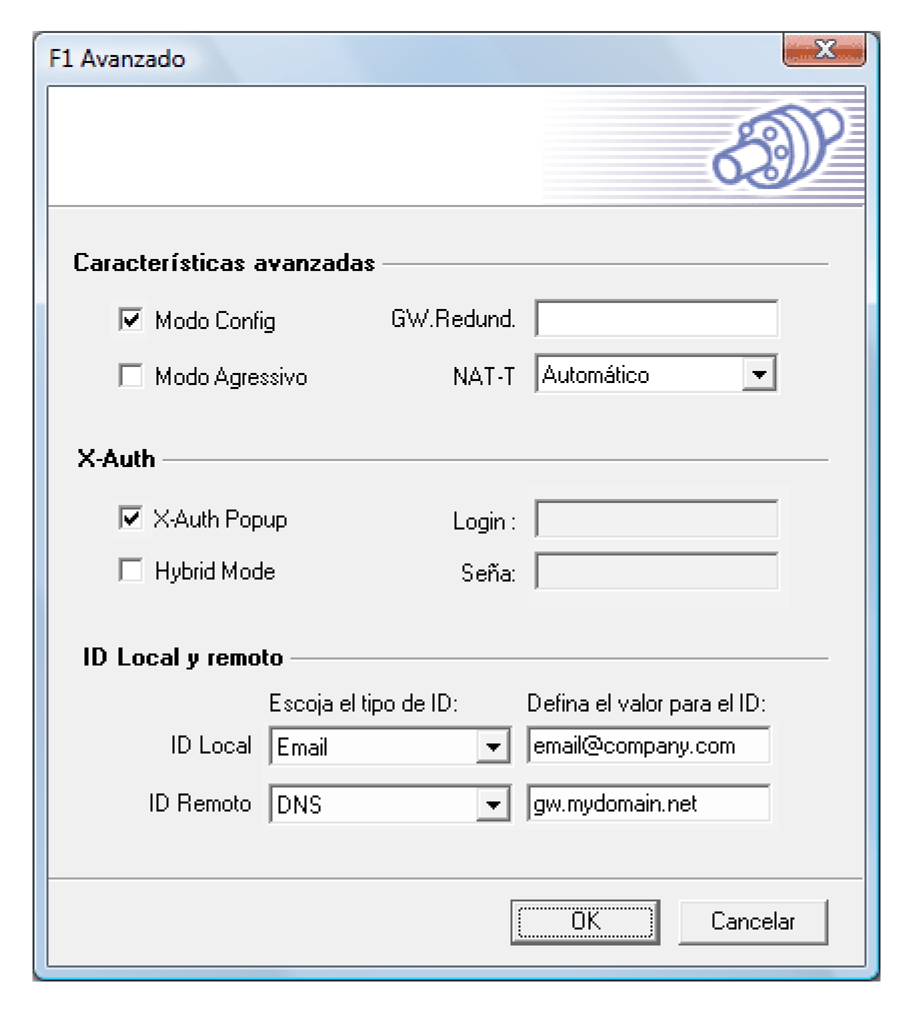
Clave secreta Contraseña o clave compartida con una gateway remota.

Certificado	Certificado X509 utilizado por el Cliente VPN. Haga clic en 'Importar Certificado' para elegir el origen del certificado: archivos PEM, archivo PKCS#21 o SmartCard (ver apartado Cómo configurar Certificados). Sólo se puede configurar un certificado por túnel.
Criptografía IKE	Algoritmo de cifrado empleado durante la fase de Autentificación (3DES, AES, ...).
Autentificación IKE	Algoritmo de Autentificación empleado durante la fase de Autentificación (MD5, SHA,…).
Grupo Clave IKE	Longitud de la clave Diffie-Hellman.

Para más parámetros avanzados, haga clic sobre 'F1 Avanzada'.

6.3.3 Descripción de los Parámetros Avanzados de la Fase 1

Para opciones y parámetros avanzados, seleccione el botón 'F1 Avanzada' en el panel de la Fase 1.



Modo Config Si está seleccionado, el Cliente VPN activará el Modo Configuración para este túnel. El Modo Configuración permite que el Cliente VPN recupere algunas informaciones sobre la Configuración VPN desde la gateway VPN. Si el Modo Configuración está seleccionado y habilitado en la gateway, se podrán negociar los siguientes parámetros entre el Cliente VPN y la gateway remota durante el intercambio IKE (Fase 1):

- Dirección IP virtual del Cliente VPN
- Dirección DNS (opcional)
- Dirección WINS (opcional)

En caso de que el Modo Configuración no esté habilitado en la gateway

	remota, tendrá que dirigirse a los parámetros 'Fase 2 Avanzada' para establecer manualmente las direcciones DNS y WINS en el Cliente VPN IPSec.
Modo Agresivo	Si está seleccionado, el Cliente VPN utilizará el modo agresivo como modo de negociación con la gateway remota.
Gateway Redundante	Permite que el Cliente VPN abra un túnel IPSec con una gateway alternativa en caso de que la primaria se haya caído o no responda. Introduzca la dirección IP o el enlace de la Gateway Redundante (por ejemplo, router.dyndns.com). • El Cliente VPN TheGreenBow contactará con la gateway primaria para establecer un túnel. Si falla tras varios intentos (por defecto, 5 intentos, configurable en el panel 'Parámetros' > "Retransmisiones"), la Gateway Redundante se utilizará como nuevo túnel final. El intervalo entre dos reintentos es de 10 segundos. • En caso de que se conecte la gateway primaria pero falle el establecimiento del túnel (por problemas de configuración VPN, por ejemplo) el Cliente VPN no intentará establecer túneles con la gateway redundante. Necesitará entonces modificar la Configuración VPN. • Si un túnel se establece satisfactoriamente en la gateway primaria con la opción DPD (Detección de Punto Inactivo) negociada por ambas partes, si la gateway primaria deje de responder (la DPD detecta gateways remotas que no responden, por ejemplo), el Cliente VPN inmediatamente se ejecuta abriendo un nuevo túnel con la gateway redundante. • El mismo comportamiento se aplicará a la gateway redundante. Esto significa que el Cliente VPN intentará abrir las gateways primaria y redundante hasta que el usuario abandone el programa o haga clic en 'Guardar y Aplicar'.
Modo NAT-T	El modo NAT-T permite los modos Forzado, Deshabilitado y Automático. El NAT-T "Deshabilitado" previene que el Cliente VPN IPSec y la gateway VPN inicien una NAT-Traversal. El modo NAT-T "Automático" permite que la Gateway VPN y el Cliente VPN negocien la NAT-Traversal. En el modo NAT-T "Forzado" el Cliente VPN IPSec TheGreenBow forzará la NAT-T mediante la encapsulación UDP de los paquetes IPSec para solucionarlo con routers NAT intermediarios.
ID Local	ID Local es la identidad que envía el Cliente VPN durante la Fase 1 a la gateway. Esta identidad puede ser: • una dirección IP (tipo = dirección IP), como por ejemplo: 195.100.205.101 • el nombre de un dominio (tipo = DNS), como mydomain.com • un dirección de correo electrónico (tipo = Email), como support@thegreenbow.es • una secuencia (tipo = ID CLAVE), como 123456 • una identificación del certificado (tipo=DER ASN1 DN) (ver configuración de Certificados). Si no se produce la identificación, se usará la dirección IP del Cliente VPN.
ID Remota	La ID Remota es la identificación que espera recibir el Cliente VPN durantela Fase 1 desde la gateway VPN. Esta identidad puede ser: • una dirección IP (tipo = dirección IP), como por ejemplo: 80.2.3.4 • el nombre de un dominio (tipo = DNS), como mydomain.com • una dirección de correo electrónico (tipo = Email), como admin.@mydomain.com • una secuencia (tipo = ID CLAVE), como 123456 • una identificación del certificado (tipo=DER ASN1 DN) (ver configuración de Certificados). Si no se produce la identificación, se usará la dirección IP del Cliente VPN.
X-Auth	Define el nombre de usuario y la contraseña de una negociación IPSec X-Auth. Si está seleccionado "X-Auth popup", una ventana emergente

	aparecerá cada vez que se requiera una autentificación para abrir un túnel con la gateway remota. Le preguntará por un nombre de usuario y una contraseña. El usuario dispone de 60 segundos (por defecto) para introducir su nombre de usuario y contraseña antes de que falle la autentificación X-Auth. Si la autentificación X-Auth falla, también lo hará el establecimiento del túnel.
Modo de Autentificación Híbrido	El modo Híbrido es un método específico de autentificación que se utiliza con la Fase 1 IKE. Este método asume una asimetría entre las entidades de autentificación. Una entidad autentifica usando claves técnicas públicas estándar (en modo de firma), mientras que otra identidad, normalmente un Usuario remoto, autentifica usando un intercambio de respuestas técnicas. Estos métodos de autentificación se emplean para establecer, al final de la Fase 1, un SA IKE con una autentificación unidireccional. Para que esta IKE sea autentificada bidireccionalmente, inmediatamente a la Fase 1 le sigue un Intercambio X-Auth [XAUTH]. El Intercambio X-Auth se utiliza para autentificar al Usuario remoto. El uso de estos métodos de autentificación es denominado modo de Autentificación Híbrido. El modo Híbrido se encuentra implementado en el Cliente VPN IPSec TheGreenBow según la RFC 'draft-ietf-ipsec-isakmp-hybrid-auth-05.txt'.

6.3.4 Modificar duración X-Auth popup

Es posible modificar la duración de visualización de la ventana X-Auth . El valor por defecto es de 60 seg. En algunos casos, podría ser interesante ampliar la duración. En esta versión del software, la modificación sólo puede hacerse en el fichero de configuración VPN con cualquier editor de texto.

Nota: Recuerde que el archivo de configuración de VPN no puede ser modificada si encriptado. Si usted necesita la protección de contraseña, modifique el parámetro de intervalo X-Auth en el fichero de configuración VPN, a continuación, Importe la configuración VPN modificada, luego vaya a 'Archivo' > 'Exportar VPN Configuración' y seleccione 'Protección de Contraseña'.

```
[General]
Shared-SADB = Defined
Retransmits = 5
Exchange-max-time = 15
Default-phase-1-lifetime = 28800,300:28800
Bitblocking = 0
Xauth-interval = 60
DPD-interval = 15
DPD_retrans = 2
DPD_wait = 15
```

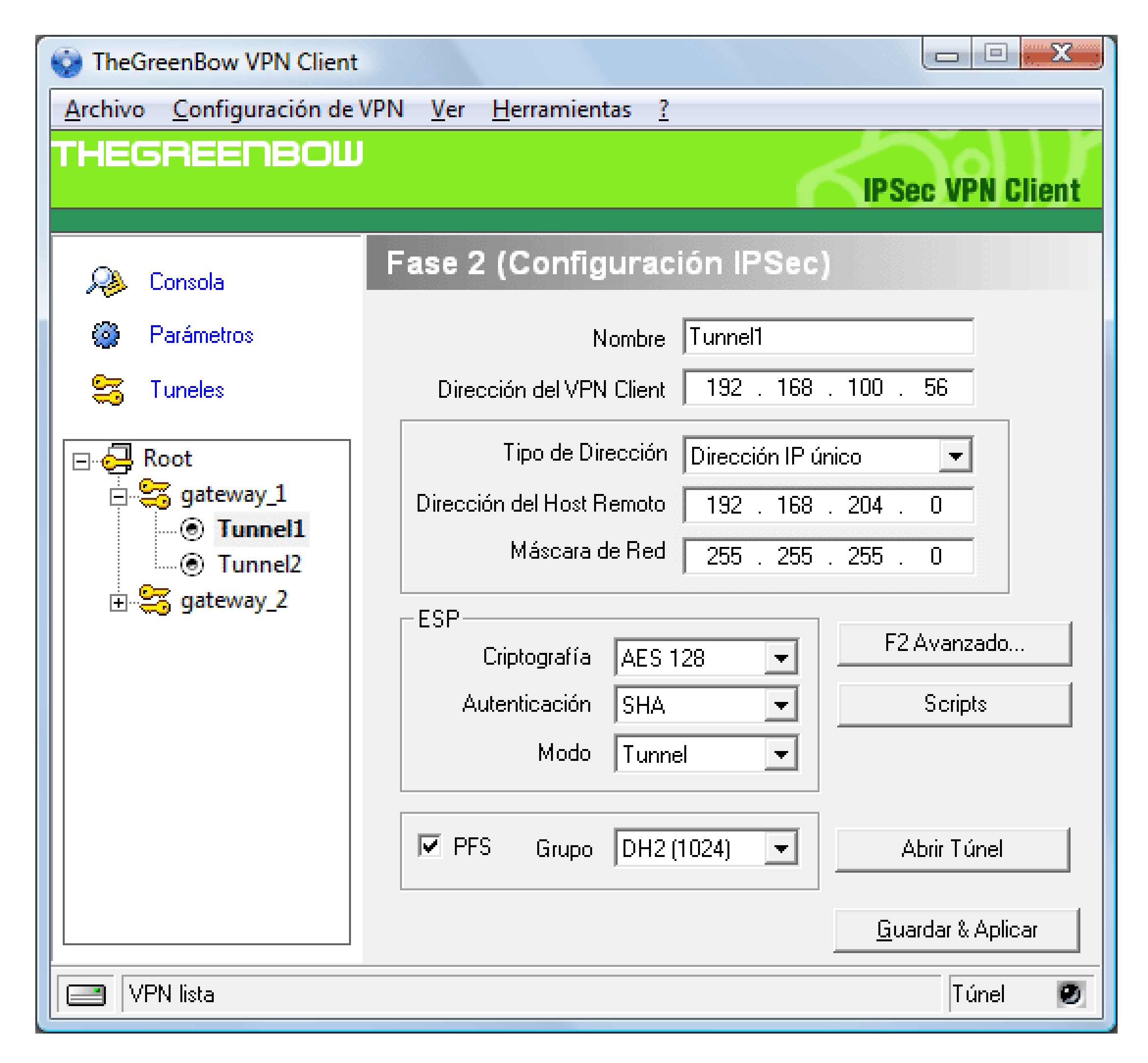
6.4 Configuración IPSec o Fase 2

6.4.1 Qué es la Fase 2?

La ventana de 'Configuración IPSec' o 'Fase 2' concierne los parámetros para la Fase 2.

El objetivo de la Fase 2 es negociar los parámetros de seguridad IPSec que se aplican al tráfico de los túneles negociados en la Fase 1.

6.4.2 Descripción de los Parámetros de la Fase 2



Nombre La etiqueta para la Configuración IPSec sólo la utiliza el Cliente VPN. Este parámetro nunca se transmite durante la Negociación IPSec. Puede cambiarle el nombre en cualquier momento y leerlo en la lista en árbol. Dos Fases no pueden tener el mismo nombre.

Dirección del Cliente VPN El Cliente VPN utiliza una dirección IP virtual dentro de la red LAN remota: El ordenador aparecerá en la red LAN con la siguiente dirección IP:
Esta dirección IP puede pertenecer a la misma subred LAN remoto (por ejemplo, en el ejemplo, usted tiene una dirección IP como 192.168.204.10) En este caso, es importante leer la siguiente nota.

Tipo de dirección El punto final remoto puede ser una red LAN o un único ordenador. Si el punto final remoto es una red LAN, elija “dirección IP de red” o “Rango de IPs”. Cuando seleccione "dirección IP de red", los dos campos "dirección de la LAN" y "Máscara de Red" aparecerán habilitados. Cuando seleccione “Rango de IP”, los dos campos “IP de Inicio” y “IP de Fin” aparecerán disponibles, permitiendo que el Cliente VPN IPSec TheGreenBow establezca un túnel sólo con un rango de direcciones IP predefinidas. El rango de direcciones IP puede ser una sola dirección IP.

Si el punto final remoto es un único ordenador, seleccione “Dirección IP Único” Cuando seleccione “Dirección IP único”, sólo aparecerá habilitado el campo “Dirección del host remoto”.

Dirección remota	Este campo puede ser “dirección de host remota" o “dirección LAN remota", dependiendo del tipo de dirección. Es la dirección IP remota o la dirección de red LAN de la gateway la que abre el túnel VPN.
Máscara de red	Máscara de subred de la red LAN remota. Sólo está disponible cuando el tipo de dirección es igual al de la “dirección de subred”.
Criptografía ESP	Algoritmo de cifrado empleado durante la fase de Autentificación (3DES, AES, ...).
Autentificación ESP	Algoritmo de autentificación negociado durante la fase IPSec (MD5, SHA, ...).
Modo ESP	Modo de encapsulación IPSec: túnel o transporte.
Grupo PFS	Longitud de la clave Diffie-Hellman.
Abrir un Túnel	Este botón permite abrir el túnel. Cambia a ”Cerrar Túnel” al abrir el túnel.
Scripts	Los scripts puede configurarse en la ventana de configuración de Script.

Nota1: La función “Rango de IP” combinada con la función 'Abrir túnel cuando haya tráfico' permite abrir automáticamente un túnel cuando se detecta tráfico para un rango específico de direcciones IP. No obstante, debe autorizar el rango de direcciones IP en la configuración de la gateway VPN.

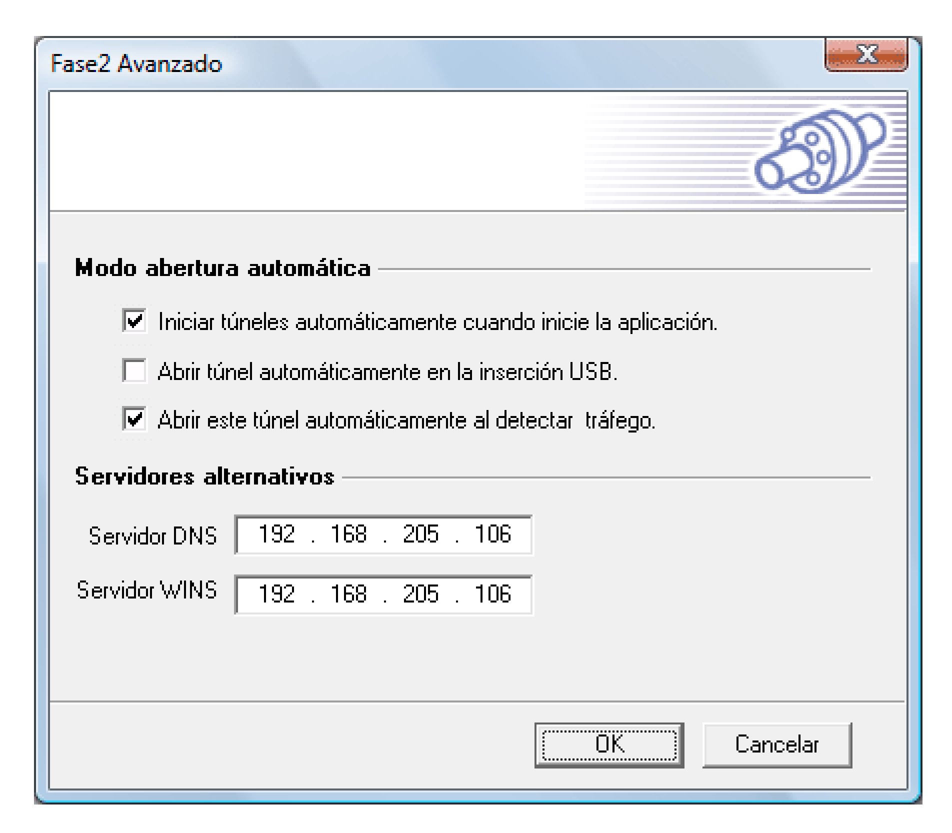
Note2: Es posible tener las dos direcciónes IP locales de su ordenador y red remote como parte de la misma subred. Para poder hacerlo, debe seleccionar "Auto abrir este túnel en la detección del tráfico" ('P2 avanzada »). Una vez que el túnel VPN se abrió en esta configuración, todo el tráfico con la red distante es permitido, pero la comunicación con la red local es imposible.

Para más parámetros avanzados, haga clic sobre 'F2 Avanzada'.

Cuando haya establecido los parámetros, haga clic en 'Guardar y Aplicar' para guardar y tener en cuenta la nueva configuración.
Encontrará un conjunto de documentos útiles para configurar el Cliente VPN disponible para cada una de
las gateways Cliente VPN que ofrecemos. Por favor, consúltelos en nuestra página web.

6.4.3 Descripción de los Parámetros Avanzados de la Fase 2

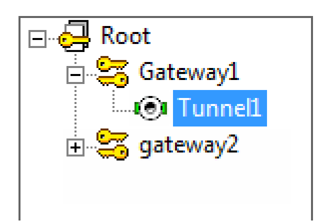
Para opciones y parámetros avanzados, seleccione el botón ‘F2 Avanzada’ en el panel de la Fase 2.



Modo Apertura Automática

El Cliente VPN puede abrir automáticamente un túnel específico (Fase2) en situaciones determinadas como:

- Abrir automáticamente este túnel cuando se inicie el Cliente VPN.
- Abrir automáticamente este túnel cuando se inserte una memoria USB (ver apartado 'Modo USB').
- Abrir automáticamente este túnel cuando el Cliente VPN detecta tráfico hacia una red LAN remota. Si está seleccionado, el icono de la Fase 2 en la lista de árbol del panel de configuración cambia su forma y color para tener en cuenta que esta función está ahora activa:

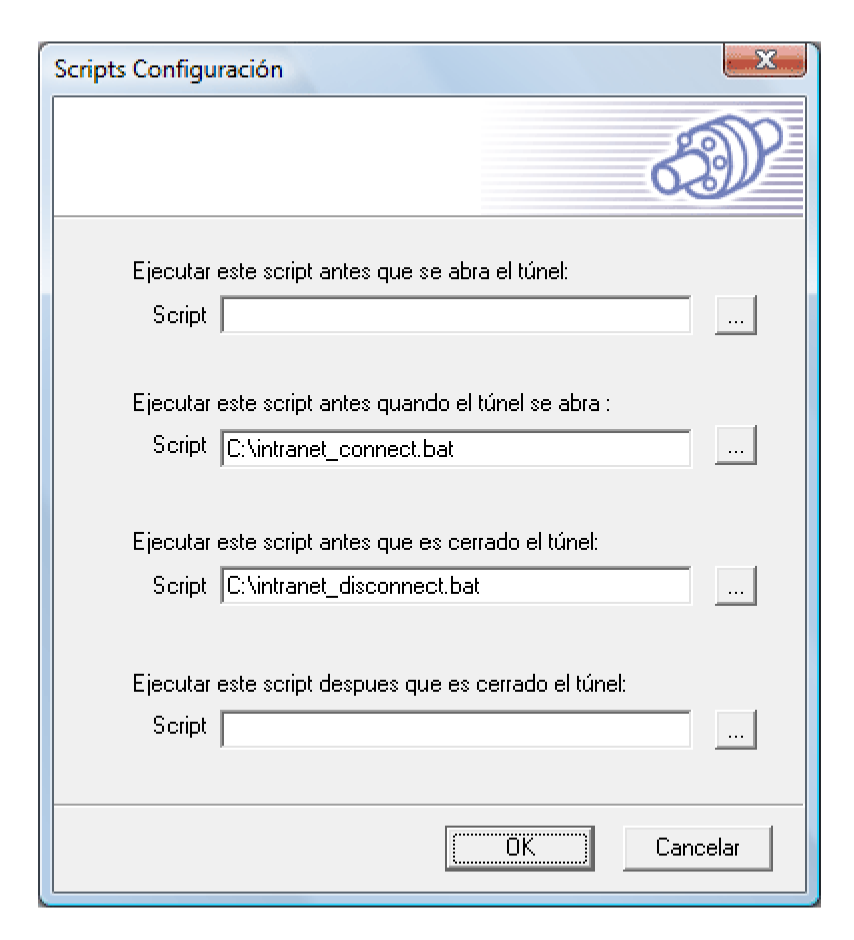


Servidores Alternativos

Las direcciones IP de los servidores DNS y WINS de una red LAN remota pueden introducirse aquí, para ayudar a resolver la dirección de los servidores de la empresa. Las direcciones DNS o WINS se toman en cuenta al abrirse el túnel y mientras esté abierto.

6.4.4 Configuración de Scripts

Los scripts pueden configurarse en la ventana de configuración de Scripts. Puede acceder a esta ventana a través del botón 'Scripts', en la ventana de Parámetros de la Fase 2.



Puede habilitar scripts o aplicaciones para cada etapa de los procesos de apertura y cierre de un túnel VPN:

- Antes abrir un túnel
- Después de abrir un túnel
- Antes de cerrar un túnel
- Después de cerrar un túnel

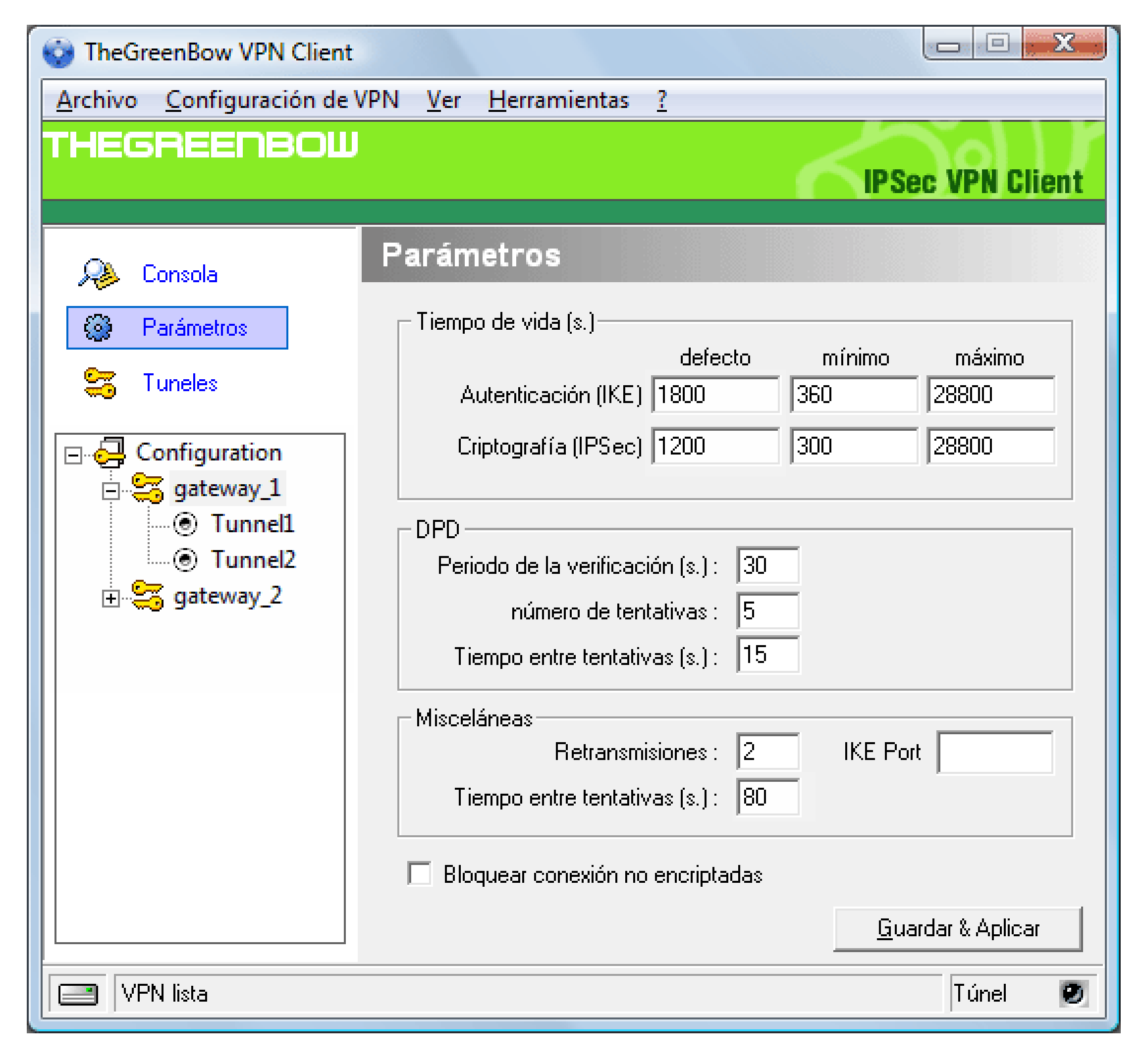
Esta opción permite ejecutar scripts (lotes, scripts, aplicaciones…) a cada paso de la conexión de un túnel para un sinfín de propósitos como, por ejemplo, verificar la versión actual del programa, la disponibilidad de la base de datos antes de abrir una aplicación de backup, si el programa está en funcionamiento, si se estableció la sesión...

También permite configurar varias configuraciones de red antes, durante y después de conectar un túnel.

6.5 Parámetros Globales

6.5.1 Descripción de los Parámetros Globales

Los Parámetros Globales son funciones genéricas que se aplican a todos los túneles VPN creados. Una vez modificados, haga clic en 'Guardar y Aplicar' para que las modificaciones se tengan en cuenta.



• **Tiempo de vida (seg.)**	**IKE lifetime por defecto**	Tiempo máximo autorizado para la autorización IKE.
	IKE lifetime mínima	Tiempo mínimo para la autorización IKE.
	IKE lifetime máxima	Tiempo máximo para la autorización IKE.
	IPSec lifetime por defecto	Tiempo máximo autorizado para la autorización IPSec
	IPSec lifetime máxima	Tiempo máximo autorizado para la autorización IPSec.
	IPSec lifetime mínima	Tiempo mínimo autorizado para la autorización IPSec.
• **Detección de Punto Inactivo (DPD)**	**Periodo de la verificación (seg.)**	Intervalo entre mensajes DPD.
	Número de tentativas	Número de mensajes DPD enviados.
	Tiempo entre tentativas (seg.)	Intervalo entre mensajes DPD cuando no responde la gateway remota.
• **Otros**	**Retransmisiones**	Número de veces que un mensaje puede ser transmitido antes de abandonar.
	Tiempo entre tentativas	Tiempo mínimo antes de cualquier intento para reiniciar la negociación IKE.
	Bloquear conexiones no encriptadas	Cuando se selecciona esta opción, sólo el tráfico cifrado está autorizado.
	IKE Port	El usuario puede cambiar el número de puerto para la negociación IKE. Los cambios aún

serán en UDP pero podrán otros puertos que no sean el 500, ya que algunos firewalls no soportan el Puerto IKE 500. La gateway remota debería soportar esta opción.

La Detección de Punto Inactivo (DPD) en una extensión IKE (Internet Key Exchange) (RFC3706) para detectar un punto IKE inactivo. El Cliente VPN IPSec TheGreenBow utiliza DPD para:

- borrar SA abiertos en el Cliente VPN cuando ha detectado un punto inactivo.
- reiniciar las negociaciones IKE con la Gateway Redundante si ha sido activada en la 'Fase 1 Avanzada' del Panel de Configuración.

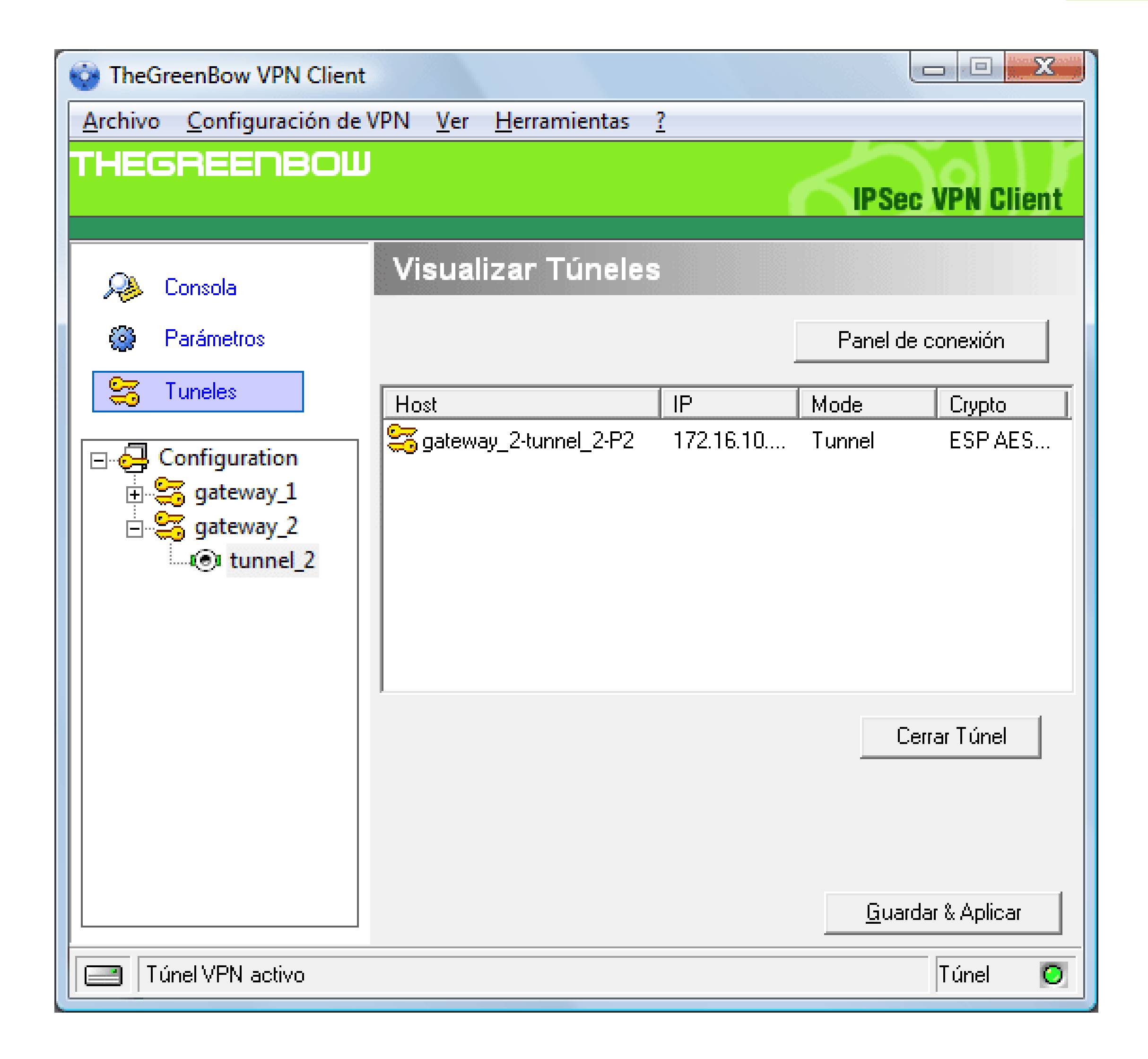
Cuando haya establecido los parámetros, haga clic en 'Guardar y Aplicar' para guardar y tener en cuenta la nueva configuración.

6.6 Administración de Túneles VPN

6.6.1 Cómo visualizar los túneles VPN abiertos?

La ventana "Visualizar Túneles" muestra los tuneles actualmente abiertos. Esta pantalla también puede ser utilizada para cerrar los túneles abiertos. Para cerra un túnel VPN, seleccione el túnel en la lista y haga clic en "Cerrar Túnel". Los túneles también pueden ser vistos, abiertos y cerrados directamente desde el menú contextual del icono de la bandeja del sistema y desde el Panel de Conexión.

Es posible cambiar de ida y vuelta entre el 'Panel de Conexión' y el 'Panel de Configuración utilizando el atajo 'Ctrl + Enter' (ver sección 'Atajos').



6.7 Modo USB

6.7.1 Qué es el modo USB?

El Cliente VPN TheGreenBow ofrece la posibilidad de securizar las configuraciones VPN y los elementos de seguridad VPN (PreShared key, Certificados,...) usando una memoria USB.

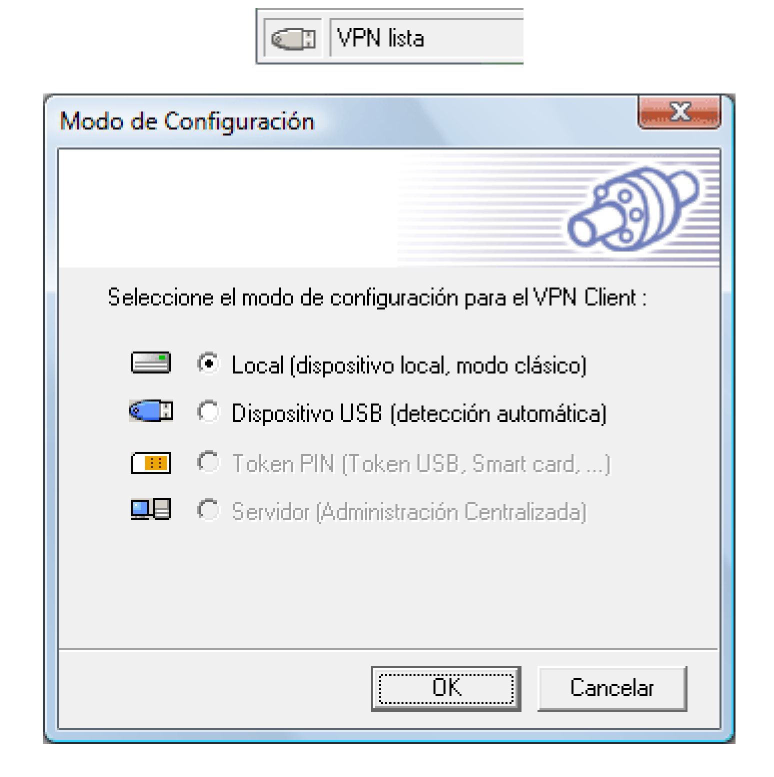
Cuando selecciona el “modo USB”, la configuración VPN y los elementos de seguridad que ésta contiene se guardan en la memoria USB al insertarla por primera vez.

Después, sólo necesitará insertar la Memoria USB para abrir túneles de manera automática. Y si desea cerrar automáticamente todos los túneles establecidos, sólo tendrá que extraer la memoria USB.

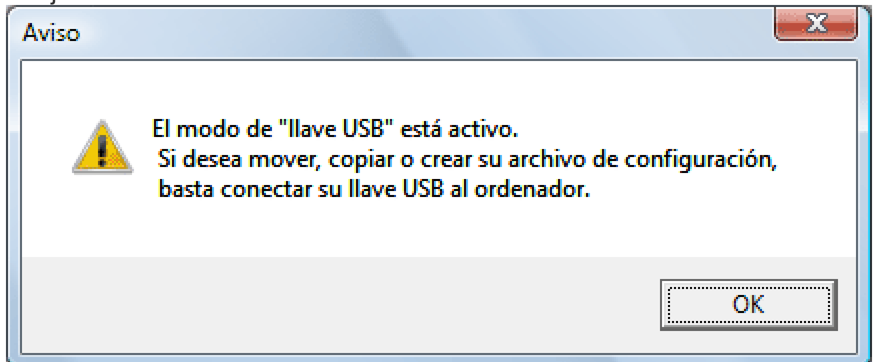
6.7.2 Como activar el modo USB?

Puede activar el Modo USB haciendo clic sobre el icono ‘Memoria USB’ en la barra de estado del Panel de Configuración o a través del menú:

- Seleccione el menú ‘Archivo’ > ‘Modo de Configuración’
- Seleccione ‘Dispisitivo USB’



Nota: En esta etapa, si el dispositivo USB ya está insertado, automáticamente reconocerá los drivers asociados con la configuración VPN. No obstante, tenga en cuenta que no es necesario insertar una memoria USB en esta etapa. Si no ha insertado ninguna memoria USB, aparecerá el siguiente mensaje:



Después de activar el modo USB, el lado izquierdo de la barra de estado mostrará un icono de memoria USB.

Cuando la memoria USB está insertada, el icono aparece en negrita: 

Cuando no hay ninguna memoria USB insertada, el icono aparece en gris:

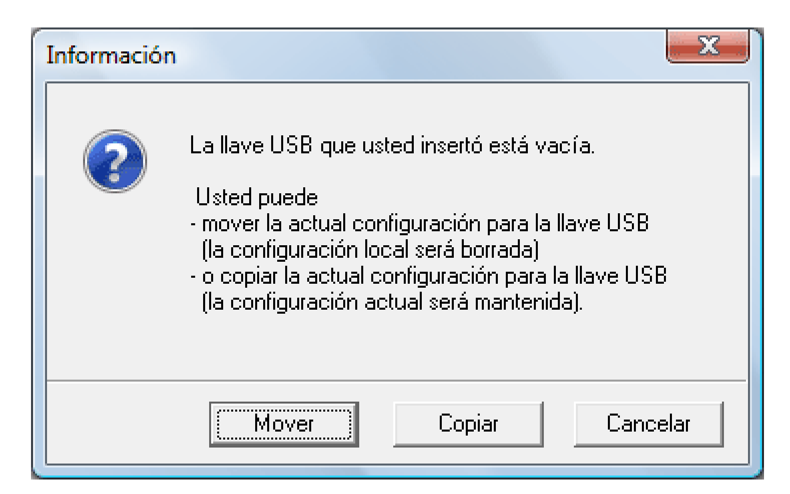

6.7.3 Cómo habilitar una nueva Memoria USB?

Puede habilitar una nueva Memoria USB copiando la configuración VPN y los elementos de seguridad en ella.

Cuando inserta una nueva memoria USB, el Cliente VPN IPSec automáticamente le propone

habilitar la memoria USB a través de las siguientes opciones:

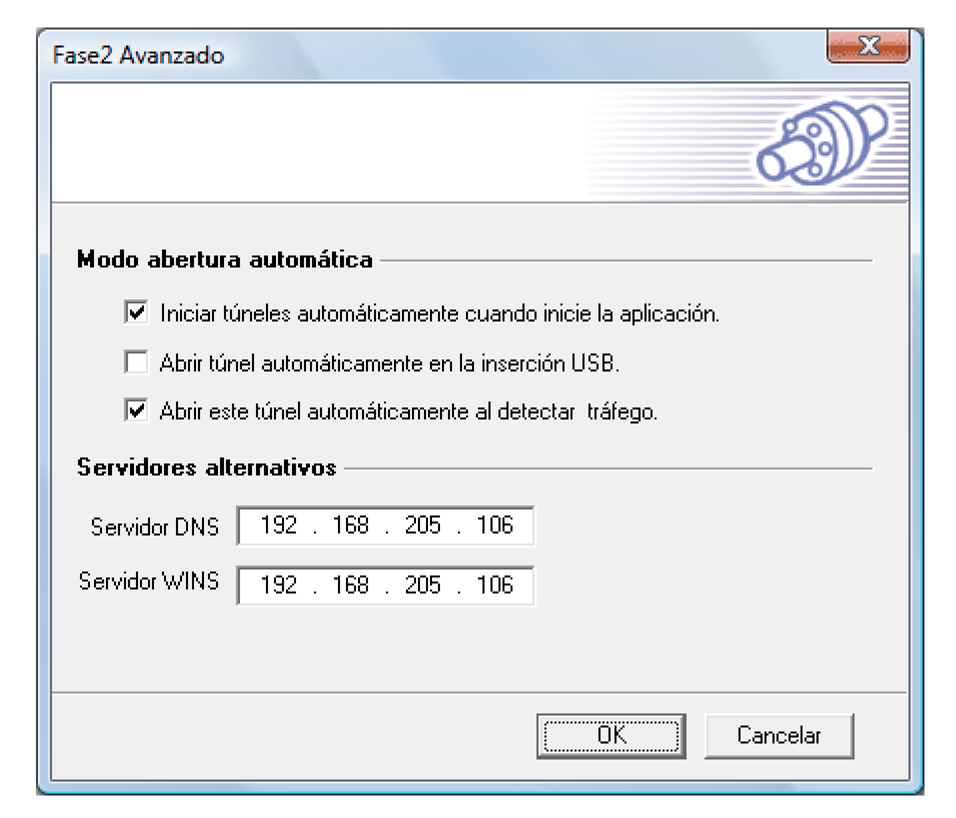
- **Copiando** la configuración VPN y los elementos de seguridad en la memoria USB: el Cliente VPN copiará la información de seguridad en la memoria USB y hará una copia en el ordenador. Esta función está especialmente diseñada para que los Informáticos habiliten con rapidez múltiples memorias USB para diversos usuarios.
- **Moviendo** la configuración a la Memoria USB: el Cliente VPN IPSec copiará la información de seguridad en la memoria USB y borrará toda la información VPN del ordenador. Este método se emplea para securizar un ordenador después de haber finalizado la instalación de una configuración VPN.



6.7.4 Cómo abrir túneles automáticamente cuando una Memoria USB está insertada?

Cada uno de los túneles debe configurarse de manera individual:

- En la Configuración IPSec (Fase 2) del túnel relevante, hacer clic sobre 'F2 Avanzada'.
- Seleccione el modo 'Abrir túnel automáticamente con la inserción USB'.



6.8 Gestión de Certificados

6.8.1 Introducción a la Gestión de Certificados

El Cliente VPN TheGreenBow puede utilizar Certificados de archivos PEM, archivo PKCS#12 o SmartCard.

Nota: El Cliente VPN TheGreenBow no permite crear Certificados. Un tercer programa tiene que crear los Certificados y almacenarlos en una SmartCard. En nuestra página webcontrará documentos de ayuda adicionales en 'Cómo generar Certificados' o 'Cómo convertir formatos de Certificado'.

6.8.2 Cómo configurar el Cliente VPN IPSec con Certificados PKCS#12?

Numerosas gateways soportan los certificados PKCS#12. El Cliente VPN IPSec TheGreenBow puede importar certificados PKCS#12 a la Configuración VPN, directamente desde la interfaz principal. Se puede definir un certificado PKCS#12 por túnel. Aún así, es posible conectar varias gateways que no utilizan el mismo PKI (Infraestructura de Clave Pública).

Para configurar el Cliente VPN IPSec con **Certificados PKCS#12**, debe seguir los siguientes pasos:

Paso 1: Seleccione el botón 'Certificado' en la ventana de la 'Fase 1' y haga clic en 'Importar Certificados…'



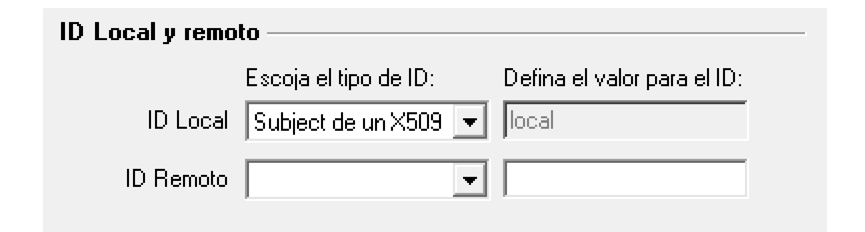
Paso 2: Seleccione de la lista 'Certificado desde un archivo PKCS#12', luego haga clic en el botón 'Importar…'

Paso 3: Seleccione el Certificado PKCS#12 que desea importar. Si el Certificado PKCS#12 está protegido, introduzca la contraseña en la ventana emergente. Una vez que el Certificado se ha importado correctamente, su asunto aparecerá automáticamente en la zona superior de la ventana 'Importar Certificados…'. Asimismo, los iconos clave identifican cada componente del certificado (certificado de raíz, certificado de usuario, clave privada) como se muestra a continuación:



Paso 4: Desde que seleccione 'Guardar y Aplicar', los Certificados PKCS#12 se almacenarán en la Configuración VPN.

Nota: Una vez que el Certificado se ha importado, su asunto se utiliza automáticamente como parámetro de la ID local de la 'Fase 1' asociada, como aparece en la ventana de la F1 Avanzada con la siguiente indicación:



6.8.3 Cómo configurar el Cliente VPN IPSec con Certificados PEM?

El Cliente VPN IPSec TheGreenBow puede importar certificados PEM a la Configuración VPN, directamente desde el Panel de Configuración. Se puede definir un certificado PME por túnel. Aún así, es posible conectar varias gateways que no utilizan el mismo PKI (Infraestructura de Clave Pública).

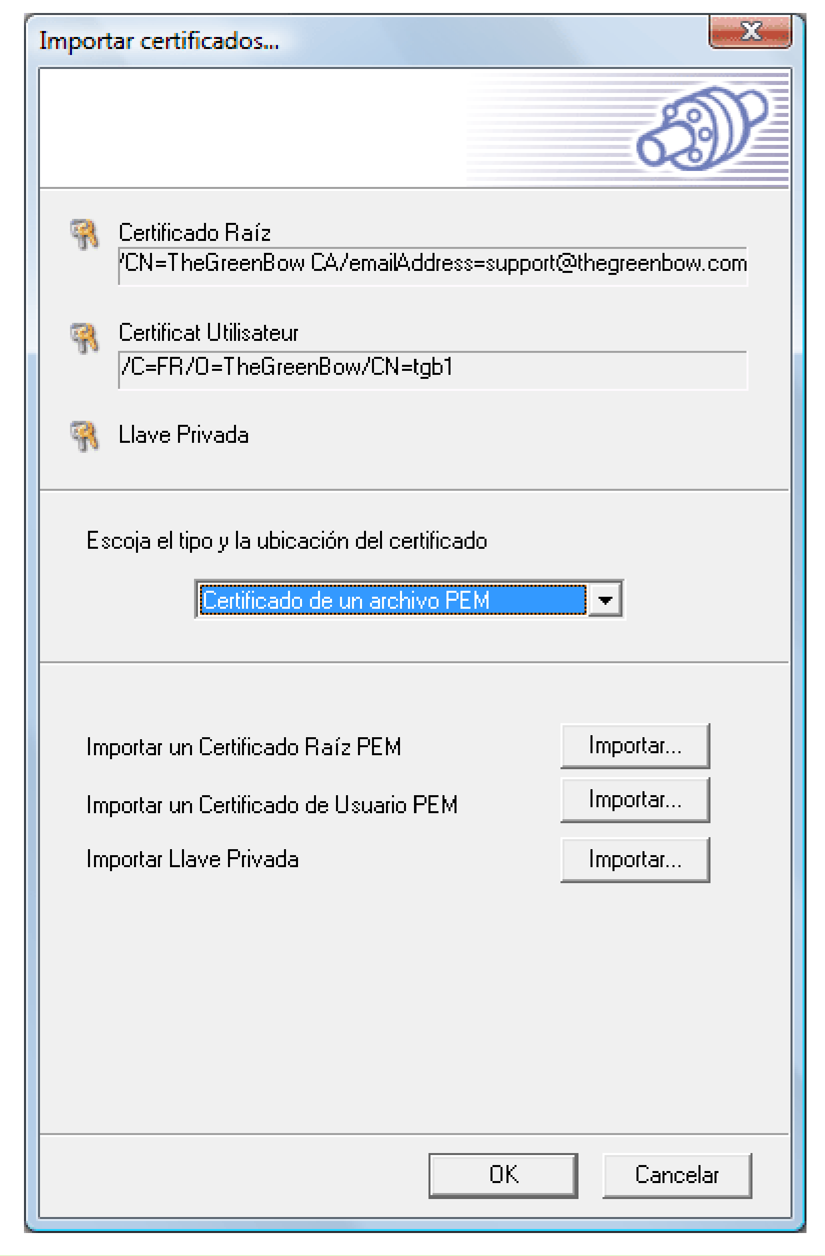
Para configurar el Cliente VPN IPSec con Certificados PEM, debe seguir los siguientes pasos:

Paso 1: Seleccione el botón 'Certificado' en la ventana de la 'Fase 1' y haga clic en 'Importar Certificados…'



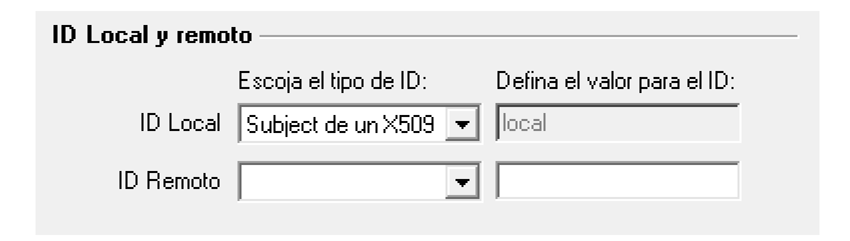
Paso 2: Seleccione 'Certificado desde un archivo PEM' en la lista.

Paso 3: Importe el Certificado de Raíz, el Certificado de Usuario y la Clave Privada haciendo clic en el
botón asociado. Una vez que el certificado se ha importado correctamente, su asunto aparecerá en la ventana 'Importar Certificados..'.



Paso 4: Desde que seleccione 'Guardar y Aplicar', los Certificados PEM se almacenarán en la Configuración VPN.

Nota: Una vez que el Certificado se ha importado, su asunto se utiliza automáticamente como parámetro de la ID local de la Fase 1 asociada, como aparece en la ventana de la 'F1 Avanzada' con la siguiente indicación:



Nota: No debe cifrar ni proteger con contraseña el archivo PEM con la clave privada.

6.8.4 Gestión de la Smart Card y Token

6.8.4.1 Cómo configurar un túnel con Certificados desde una SmartCard?

El Cliente VPN IPSec TheGreenBow puede leer Certificados desde Smart Cards. Puede utilizar las Smart Cards para securizar certificados X509 que puedan estar protegidos con un código PIN.

Para configurar un túnel usando Certificados desde Smart Cards, debe seguir los siguientes pasos:

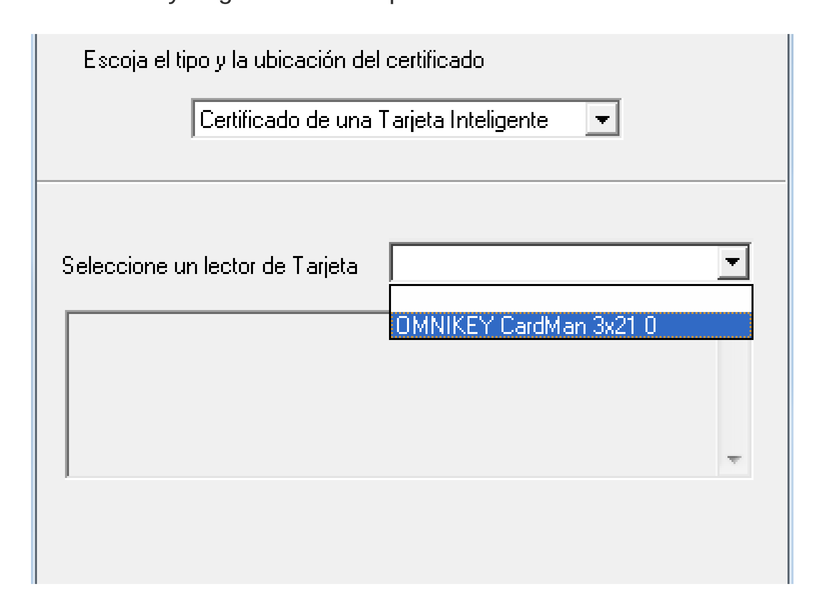
Paso 1: Seleccione el botón 'Certificado' en la ventana de la 'Fase 1' y haga clic en 'Importar Certificados…'



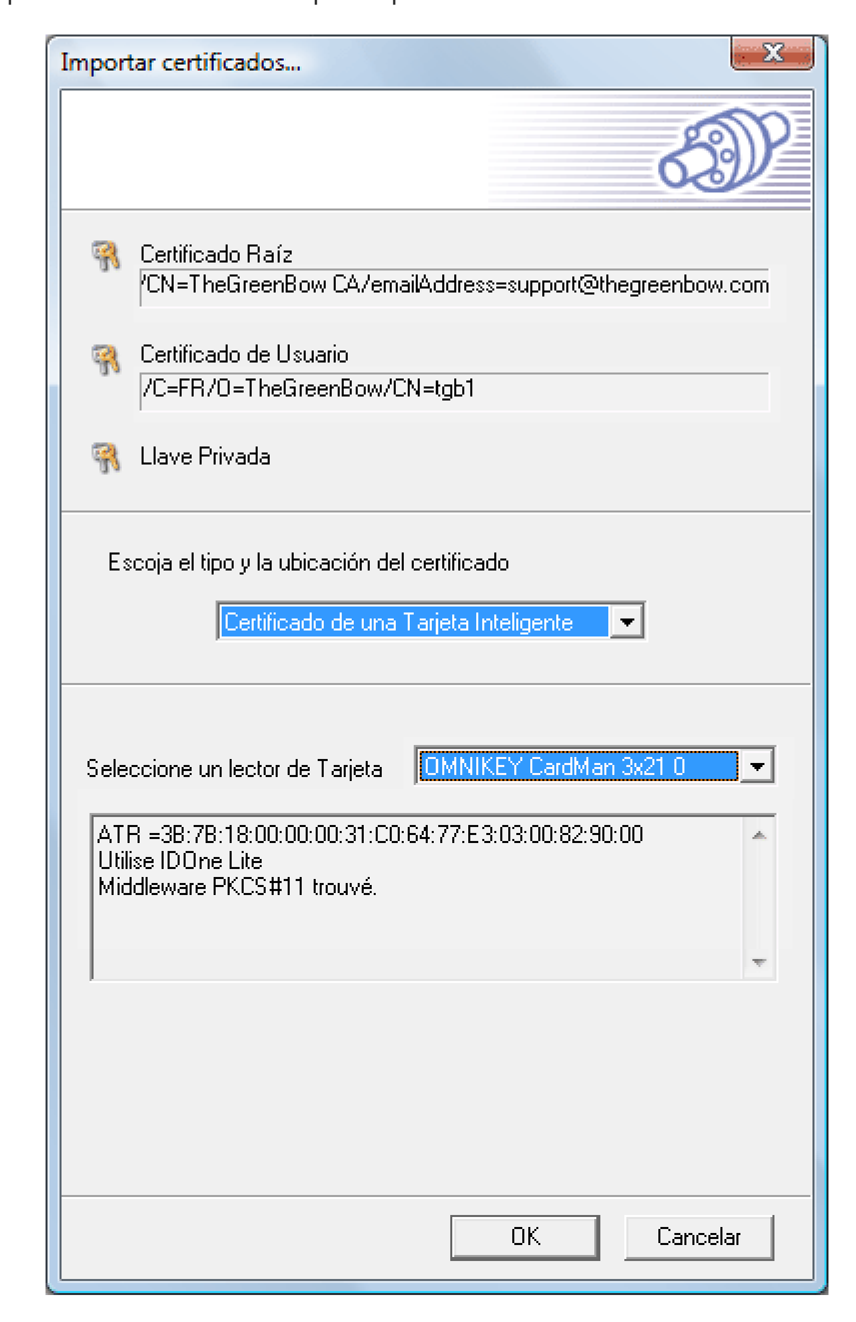
Paso 2: Seleccione 'Certificado desde una SmartCard' de la lista. Aparecerá una lista de Lectores de SmartCard en la parte inferior de la ventana.



Paso 3: Seleccione el Lector de SmartCard que desea utilizar. Se inicia el proceso de identificación del Lector de SmartCard y puede que sea necesario un código PIN. Introduzca el código PIN de la SmartCard y haga clic en 'Aceptar'.



Después de leer satisfactoriamente la SmartCard, aparecerá la información acerca del Lector de SmartCard y de la SmartCard en el cuadro de texto bajo la lista. Los asuntos de los Certificados, en cambio, aparecerán en los dos campos superiores de la ventana.



Paso 4: Desde que seleccione 'Guardar y Aplicar', la información del Lector de SmartCard se almacenará en la Configuración VPN.

6.8.4.2 Cómo utilizar un túnel con Certificados desde una SmartCard?

Cuando un túnel está configurado para utilizar Certificados desde una SmartCard, solicitará que el usuario introduzca el código PIN de la SmartCard cada vez que tenga que abrir el túnel (excepto en renegociaciones VPN automáticas).

Así, para abrir un túnel con Certificados desde una SmartCard, deberá disponer de:

1. El lector de SmartCard correctamente instalado y configurado en el Cliente VPN IPSec
2. Una SmartCard legible insertada en el lector de SmartCard
3. El código PIN correcto para leer la SmartCard.

Cada problema que surja al usar la SmartCard aparecerá en la Consola del Cliente VPN IPSec. Ver el siguiente apartado: 'Problemas con SmartCard'.

6.8.4.3 Problemas con SmartCard

Los usuarios pueden encontrarse con errores durante la configuración de la SmartCard y de los Lectores de SmartCard.

Problema con SmartCard	Messaje (*)
No se encuentra ningún Lector de SmartCard	No smart card found
Si no se ha encontrado ninguna SmartCard, probablemente sea porque el Lector de SmartCard middleware no se encuentre. La forma más sencilla de añadir un Lector de SmartCard middleware aparece en el texto en la parte inferior de la lista.	No ATR Unknown ATR: this smart card may not be supported. No PKCS#11 middleware for this smart card was found. You can set PKCS#11 middleware with the command line: Vpnconf.exe /addmiddleware:path_to_the_dll
No se puede leer la SmartCard	ATR = 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00 Using IDOne Lite PKCS#11 middleware found Error 0x00000015
El código PIN es incorrecto	ATR = 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00 Using IDOne Lite PKCS#11 middleware found Wrong PIN code
No se encontró ningún certificado en la SmartCard	ATR = 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00 Using IDOne Lite PKCS#11 middleware found No configuration or no certificate found in the smart card

(*) Este mensaje aparece en el campo de texto inferior de la lista de Smart Card.

Users may encounter issues while opening a tunnel which requires Certificates on a SmartCard.

Problema con Smart Card	Mensaje de la Consola
No se encuentra ningún Lector de SmartCard	Missing SmartCard Reader
El código PIN es incorrecto	Wrong PIN code
No se ha encontrado ningún certificado en la SmartCard o no se puede leer la SmartCard	Empty or unreadable SmartCard

6.9 Gestión de las Configuraciones VPN

6.9.1 Importar o Exportar una Configuración VPN desde el menú

El Cliente VPN TheGreenBow puede importar o exportar una Configuración VPN. Con esta opción, los Informáticos pueden preparar una configuración y repartirla a otros usuarios.

- Para importar una configuración, seleccione el menú "Archivo > Importar Configuración VPN".
- Para exportar una configuración, seleccione el menú "Archivo > Exportar Configuración VPN".

Todos los archivos de configuración VPN tendrán una extensión ".tgb".

Puede proteger con contraseña la Configuración VPN que incluya Certificados durante la importación o exportación. Cuando el usuario desea exportar una configuración, automáticamente una ventana le preguntará si quiere proteger o no la configuración VPN



Cuando una Configuración VPN está protegida con contraseña, al importarla, automáticamente exigirá que el usuario introduzca la contraseña. Una Configuración VPN exportada que no está protegida con contraseña se importará automáticamente sin pedir nada al usuario.

Nota: Importar/Exportar en 'Modo USB'
Cuando el Cliente VPN está configurado en "Modo USB" y está insertada una memoria USB, la importación de una Configuración VPN se escribirá directamente en la memoria USB. Si el Cliente VPN está configurado en "Modo USB" pero no hay ninguna memoria USB insertada (el icono USB en la parte inferior izquierda está en gris), la exportación y la importación de una Configuración VPN aparecerán deshabilitadas.

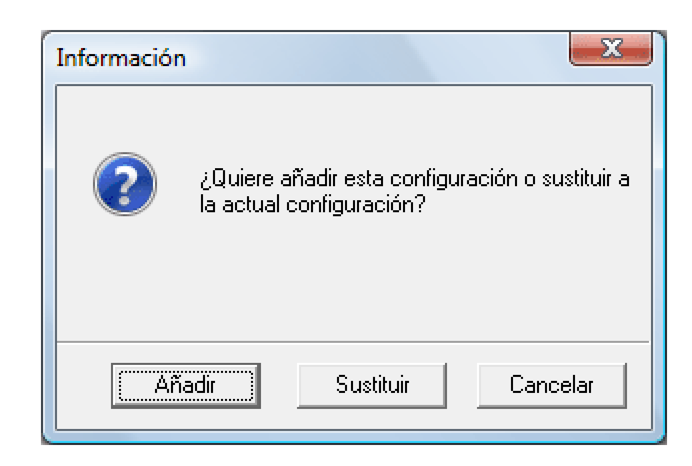
Nota: También puede importar una Configuración VPN a través de la línea de comandos.

6.9.2 Fusionar Configuraciones VPN

El Cliente VPN IPSec TheGreenBow puede importar uno o varios túneles existentes en una configuración VPN. Con esta función, los administradores pueden fusionar una nueva configuración VPN con un nuevo Enrutador en una configuración VPN existente y ofrecer a los usuarios o a un grupo de usuarios.

Fusionar Configuraciones VPN puede se hacer de varias maneras.

1. Importar nueva Configuración VPN via menu 'Archivo'>'Importar Configuración VPN' y seleccionar 'Add' en vez de 'Replace'.



2. Arrastre y suelte una nueva configuración VPN en el programa con una configuración VPN existente e ya iniciadas. Exactamente la misma ventana (véase más arriba) aparecerá preguntando si el usuario quiere 'Añadir' o 'Reemplazar' la configuración VPN existente.

3. Importar nueva Configuración VPN en lineas de comando.

   " **`[path]\vpnconf.exe /add:[file.tgb]`** " donde **`[path]`** es el directorio de instalación del Cliente VPN, y [file.tgb] es el archivo de configuración VPN. Este comando no maneja rutas relativas (por ejemplo, ".. \ .. \ file.tgb"). Para más detalles, véa la sección importar lineas de comando.

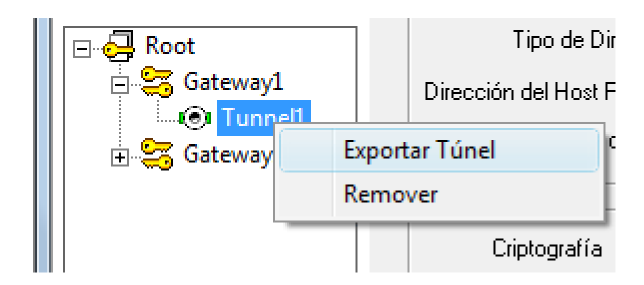
De cualquier manera que elija importar una configuración VPN, aquí estan comportamientos comunes:

- Global parameters no son importados en el caso de al menos un túnel ya estaba configurado antes de la importación y el usuario selecciona "Añadir" Configuración VPN en la ventana emergente.
- Global parameters son importados en el caso del usuario seleccionar "Replace" o se ningún túnel ya estaba configurado antes de la importación.
- Conflict con los nombres de túneles entre los actuales y los importados se resuelven automáticamente por el programa informático mediante la adición de un incremento entre el brazo por ejemplo, tunnel_office (1) para los nombres de tuneles importados (es decir, tanto Phase1 y la Fase 2).

6.9.3 Dividir Configuración VPN

El Cliente VPN IPSec TheGreenBow puede exportar un túnel de una configuración VPN existentes. Con esta función, los administradores de TI pueden dividir configuración VPN existentes en pequeñas Configuraciones VPN y entregarlo a los usuarios o grupo de usuarios Para exportar un túnel sólo, debe seguir los siguientes pasos:

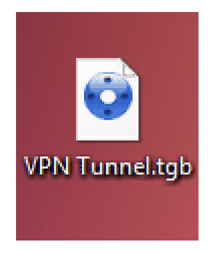
1. Haga clic derecho sobre cualquier túnel de la Fase 2 de su Configuración VPN, y seleccione "Export Túnel '.



2. Una ventana aparecerá para pedir sobre la protección con contraseña de la configuración VPN.



3. Una vez exportada, la configuración VPN puede ser enviada a los usuarios o puede hacer doble clic sobre él para iniciar el Cliente VPN IPSec TheGreenBow.



Nota:

- Con la exportación de la Fase 2 se asocia la exportación de la Fase 1 también. Esto significa también la exportación de certificados que podría haber sido definido en esta Fase 1.
- La exportación de la Fase 2 exportará los Global Parameters también.

6.9.4 Incrustar su propia Configuración VPN en la Instalación del Cliente VPN IPSec

Puede incrustar una Configuración VPN (creada con anterioridad) en la Instalación del Cliente VPN IPSec. lo que permite que el Informático distribuya el software del Cliente VPN IPSec preconfigurado en un único pack a todos los usuarios de la compañía.

6.9.5 Configuración VPN por defecto

La Instalación del Cliente VPN IPSec incluye una Configuración VPN por defecto. Esta Configuración VPN por defecto permite abrir un túnel con la demo del servidor TheGreenBow al

instalar el Cliente VPN IPSec.

Esto es especialmente útil para comprobar si puede abrir un túnel desde su ordenador a una red remota operativa para análisis y eventualmente para depuraciones.



Implementación

7 Implementación

7.1 Configuración VPN Incrustada

Durante la instalación del programa, el Cliente VPN IPSec importa automáticamente un archivo de Configuración VPN ".tgb" incrustado en la Instalación del Cliente VPN IPSec (descomprimido, ver la descripción 'Guía de Despliegue' disponible en nuestra página web).

El proceso para crear una instalación con una Configuración VPN es el siguiente:

- Crear la Configuración VPN que tiene que incrustarse en la Instalación. Este paso debe realizarse desde un Cliente VPN IPSec previamente instalado, desde donde se ha exportado la Configuración VPN y se ha nombrado 'myconfig.tgb', por ejemplo.
- Crear una instalación silenciosa, o simplemente descomprimir la Instalación del Cliente VPN IPSec.
- Añadir la Configuración VPN "myconfig.tgb" en el directorio de instalación descomprimido.
- Implementar el paquete al usuario (la configuración VPN "myconfig.tgb" se utilizará durante la instalación)

Nota importante: la Instalación no puede importar y usar una Configuración VPN cifrada (protegida). Cuando crea la Configuración VPN, asegúrese de que la exporta sin cifrarla, es decir, sin protegerla con contraseña.

7.2 Opciones de Instalación

7.2.1 Introducción a las opciones de Instalación

Numerosas opciones están disponibles con la Instalación del Cliente VPN IPSec.

1. Configuración de la Interfaz gráfica de Usuario: '*full*', '*user*' o '*hidden*' ('completa', 'usuario' u 'oculta'.)
2. Protección del control de acceso a la Interfaz gráfica de Usuario con contraseña
3. Configuración de los elementos de la bandeja del sistema.
4. Otras opciones para el Inicio del programa, el Número de Licencia, Auto Activación del Software, no ventana de evaluación, idiomas y el correo electrónico para la Activación.

Sintaxis:

```
Setup.exe /S --license=0123456789ABCDEF0123 --start=1
--activmail=smith@smith.com
```

Atención: las opciones '**--guidefs**', '**--menuitem**', '**--license**', '**--start**', '**--activmail**', '**--password**', '**--autoactiv**', '**--noactivwin**', '**--lang**' solo se podrán usar con la función '/S' (instalación modo silencioso, case sensitive).

Para más detalles, por favor consulte el 'Guía de Despliegue' en nuestra página web.

7.2.2 Opción de Instalación para la Interfaz de Usuario

Sintaxis: **--guidefs=full|user|hidden**
permite definir la apariencia de la Interfaz de Usuario cuando se inicia el Cliente VPN IPSec.

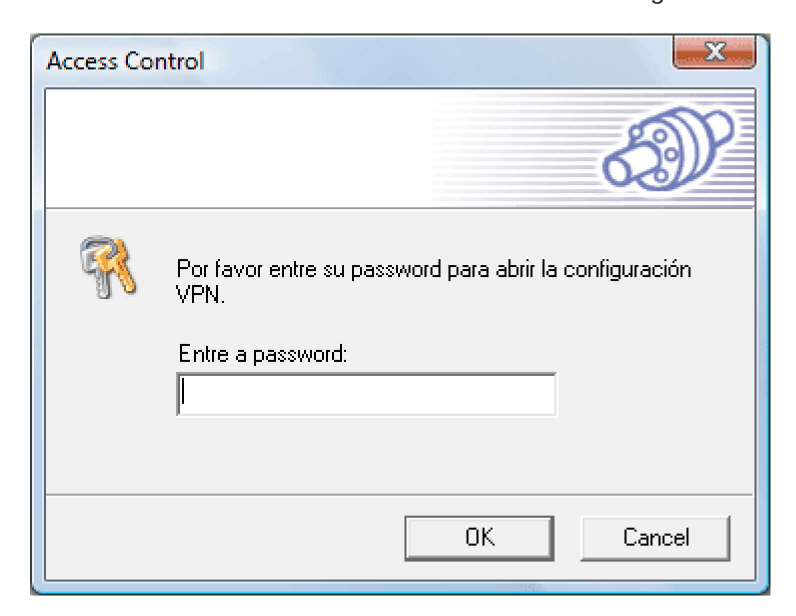
"full": [Defecto] Aparece el Panel de Configuración..
"user": Aparece el Panel de Conexión.
"hidden": No aparece el Panel de Configuración VPN ni el Panel de Conexión. Sólo se puede abrir el menú de la bandeja del sistema. Los túneles se pueden abrir desde la bandeja del sistema.

7.2.3 Opción de Instalación para el control de acceso a la Interfaz de Usuario

Sintaxis: **--password=mypwd**
Permite controlar el acceso a la Interfaz de Usuario VPN con contraseña.

Le pedirá la contraseña al usuario:

- Cuando haga clic o doble clic en el icono Cliente VPN en la bandeja del sistema.
- Cuando desea cambiar del Panel de Conexión al Panel de Configuración.



Ejemplo: **--guidefs=user --password=admin01**
Estas dos opciones permiten bloquear la Interfaz de Usuario sólo en el “Panel de Conexión”, mientras que
el acceso al Panel de Configuración está protegido con contraseña.

7.2.4 Opción de Instalación para los elementos de la bandeja del sistema

Sintaxis: **--menuitem=[0...31]**
Permite especificar los elementos de la bandeja del sistema que el Responsable Informático quiere mantener.

El valor es un 'campo de bits' ('bitfield'): **1 = Salir, 2 = Panel de Conexión, 4 = Consola, 8 = Guardar y Apllicar, 16 = Panel de Configuración, Por Defecto es 31: Todos los menus..**

Ejemplo: **--menuitem=5** configurará la bandeja del sistema con los elementos: Salir + Consola.

Nota 1: Los túneles siempre aparecen en la bandeja del sistema y pueden abrirse y cerrarse desde el menú de la bandeja del sistema..

Nota 2: **'menuitem'** y **'guidefs=hidden'**.

Por defecto, **`guidefs=hidden`** limita el menú de la bandeja del sistema a Salir + Consola. (Los elementos 'Guardar y Aplicar' y 'Panel de Conexión' no están visibles). No obstante, el uso de **`'menuitem'`** es prioritario al de **`'guidefs'`**.
Lo que significa: **`"--guidefs=hidden --menuitem=1"`** establecerá el menú de la bandeja del sistema solamente con el elemento 'Salir'.

7.2.5 Otras opciones de Instalación

Las otras líneas de comando para la instalación son:

Sintaxis: **`--license=[licence_number]`**
Permite configurar el número de licencia. El Número de Licencia es un conjunto de 24 caracteres hexadecimales. Los Números de Licencia antiguos pueden tener 20 caracteres hexadecimales.

Sintaxis: **`--start=[1|2|3]`**
Permite configurar el modo de inicio del Cliente VPN: después de iniciarse windows [1], durante el arranque [3], o manualmente [2] . [1] está configurado por defecto.

Sintaxis: **`--activmail=[activation_email]`**
Permite forzar el correo electrónico utilizado para la confirmación de la activación. Durante el proceso de activación, la ventana de diálogo que se utilizó para introducir el correo electrónico aparecerá deshabilitada.

Sintaxis: **`--autoactiv=1`**
En el caso de una actualización del software (es decir, número de licencia y la activación de correo electrónico ya han sido inscritas en una instalación anteriore) y la opción --autoactiv=1 es añadida, el software va a tratar de activar el software automáticamente cuando se inicia si la red está disponible o cuando se solicite la apertura de un túnel si la red no estaba disponible al inicio..

Sintaxis: **`--noactivwin=1`**
No visualización de la "ventana de prueba 'una vez iniciado el software hasta que finalice el período de prueba. El usuario no sabe que está en período de prueba y el software se desactivará al final del período de prueba. Esto significa que si el usuario intenta poner en marcha el software después de la clausura del período de prueba, el software lanzara la "ventana de prueba", pero el botón 'Evaluate' botón estará desactivado.

Sintaxis: **`--lang=[código de idioma]`**
Esta opción especifica el idioma para el software y para la instalación del software Cliente VPN IPSec TheGreenBow. Los idiomas disponibles se enumeran a continuación.

ISO 639-2 code	código de idioma	Nombre en Inglés
EN	1033 (default)	English
FR	1036	French
ES	1034	Spanish
PT	2070	Portuguese
DE	1031	German
NL	1043	Dutch
IT	1040	Italian
ZH	2052	Chinese simplified
SL	1060	Slovenian
TR	1055	Turkish

PL	1045	Polish
EL	1032	Greek
RU	1049	Russian
JA	1041	Japanese
FI	1035	Finnish
SR	2074	Serbian

Ejemplo:
```
Setup /S --license=0123456789ABCDEF0123 --start=1
--activmail=smith@smith.com
```

7.3 Línea de comandos

7.3.1 Opciones de la línea de comandos

Varias líneas de comando están disponibles, que están destinados a ser utilizados por los administradores de TI para adaptar el Cliente VPN IPSec a sus necesidades y contribuir a la integración con otras aplicaciones.

- Importar o Exportar una Configuración VPN
- Abrir o Cerrar un Túnel VPN

Para más detalles, por favor consulte el 'Guia de Despliegue' en nuestra página web.

7.3.2 Detener el Cliente VPN IPSec: opción "/stop''

El Cliente VPN TheGreenBow puede detenerse en todo momento con la línea de comando:

" [path]\vpnconf.exe /stop " donde **[path]** es el directorio de instalación del Cliente VPN IPSec.

Si existen varios túneles activos, se cerrarán automáticamente.

Esta función es útil, por ejemplo, en un script que arranca el Cliente VPN después de establecer una conexión dial up y lo cierra justo antes de la desconexión.

7.3.3 Importar o Exportar una Configuración VPN

El Cliente VPN TheGreenBow puede importar una determinada configuración mediante la línea de comando:

" [path]\vpnconf.exe /import: [file.tgb] " donde **[path]** es el directorio de instalación del Cliente VPN, y **[file.tgb]** es el archive de la Configuración VPN. Este comando no soporta rutas relativas ("…\ .. \archivo.tgb", por ejemplo). Double-quotes are supported allowing paths containing spaces.

" /import: " puede utilizarse con el Cliente VPN IPSec en funcionamiento o no. Cuando el Cliente VPN ya está iniciado, importa de manera dinámica la nueva configuración y la aplica automáticamente (reinicio el servicio IKE). Si no se ha iniciado el Cliente VPN, arrancará con la nueva configuración.

" /importonce: " permite importar una configuración VPN sin que el Cliente VPN esté en funcionamiento. Este comando es especialmente útil para la instalación de scripts ya que permite arrancar una instalación silenciosa e importar la configuración automáticamente.

" /export: " permite exportar la actual Configuración VPN (incluyendo los certificados) en un archivo específico. Este comando funciona cuando aún no se ha iniciado el Cliente VPN. No soporta rutas relativas ("…\ .. \archivo.tgb", por ejemplo).

" /exportonce: " permite exportar la actual Configuración VPN (incluyendo los certificados) en un archivo específico. Este comando no funciona si no se ha iniciado el Cliente VPN.

" **/replace:** " permite sustituir la actual configuración por una nueva configuración VPN. Esta función está disponible en la versión del programa 4.1 y mayores, y puede ser utilizada en lugar de la opción /importonce para importar un archivo de configuración VPN sin correr el Cliente VPN.

" **/add:** " permite importar una nueva configuración de VPN en una configuración VPN existente y fusiona ambas en una sola configuración VPN. Esta línea de comandos puede ser utilizado tanto si el Cliente VPN está funcionando o no. Este comando no inicia el Cliente VPN si no está ejecutando ya.

" **/pwd:[password]**" permite establecer una contraseña para operaciones de importación. Esta opción debe usarse junto con la opción /import o /importonce.

Los 6 argumentos **"import"**, **"importonce"**, **"export"**, **"exportonce"**, **"replace"** y **"add"** son exclusivos y no pueden utilizarse conjuntamente.

7.3.4 Abrir o Cerrar un Túnel VPN

El Cliente VPN TheGreenBow puede abrir o cerrar un túnel en línea de comando. Ambas líneas de comando se puede invocar cuando el Cliente VPN IPSec TheGreenBow está lanzado:

" **[path]\vpnconf.exe /open:[phase1-phase2]** " donde **[path]** es el directorio de instalación de Cliente VPN, y **[phase1-phase2]** son los nombres de la Fase1 y de la Fase2 en el fichero de la Configuración VPN. Este comando no maneja rutas relativas (por ejemplo "..\..\file.tgb"). Comillas dobles son soportadas lo que permite caminos que contengan espacios.
En caso de que el túnel ya está abierto, esta línea de comando no tiene efecto.

" **[path]\vpnconf.exe /close:[phase1-phase2]** " donde **[path]** es el directorio de instalación de Cliente VPN, y **[phase1-phase2]** son los nombres de la Fase1 y de la Fase2 en el fichero de la Configuración VPN. Este comando no maneja rutas relativas (por ejemplo "..\..\file.tgb"). Comillas dobles son soportadas lo que permite caminos que contengan espacios.
En caso de que el túnel ya está cerrado, esta línea de comando no tiene efecto.

Ambos argumentos "**open**" y "**close**" son exclusivas y no se pueden usar juntos.

Nota de Restricción:
- La ejecución de esas líneas de comando abrirá la interfaz gráfica de usuario del Cliente VPN. Esta restricción será corregida en una próxima versión del programa.

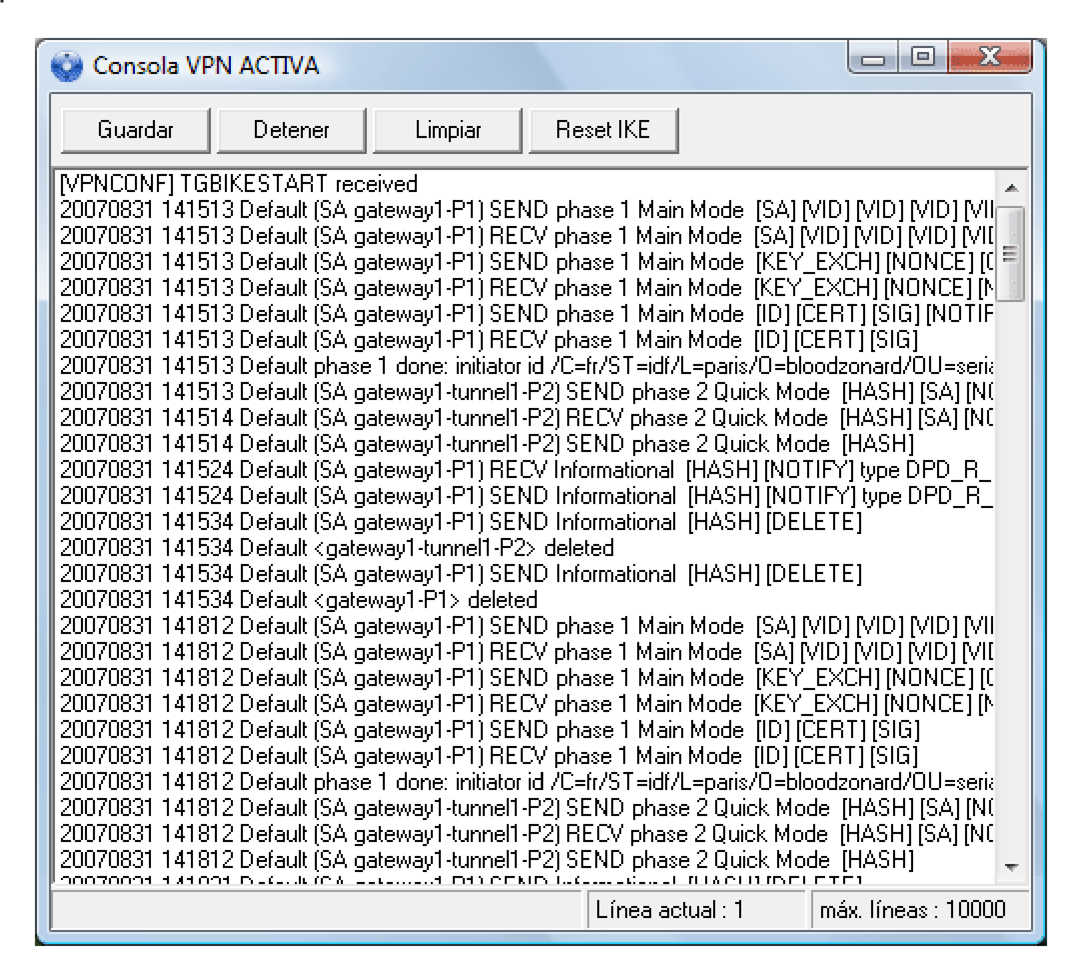


Consola y Registros

8 Consola y Registros

8.1 Consola

La ventana 'Consola' está disponible desde el menú contextual del icono del systray o del button 'Consola' en el Panel de Configuración. Esta ventana puede utilizarse para analizar los túneles VPN. Esta herramienta es particularmente útil para los administradores de TI en la creación de su red.



Button	**Descripción**
Guardar	Guardar los registros actuales en un archivo. Futuro registros no se guardan en el archivo seleccionado.
Detener	Start/Stop los registros
Limpiar	Limpiar la Consola.
Reset IKE	Reinicia el proceso IKE.



Localización del Software

9 Localización del Software

La localización (L10N) del Cliente VPN IPSec es ahora totalmente posible. Todas las secuencias que utiliza el Cliente VPN están recogidas en una herramienta de Traducción, listas para ser traducidas.

Paso 1: Descargue la herramienta de Traducción del Cliente VPN desde nuestra página web.
Paso 2: Traduzca las secuencias a su idioma
Paso 3: Envíe la traducción del Cliente VPN a: support@thegreenbow.es
Paso 4: Incluiremos su idioma en la siguiente versión del Cliente VPN IPSec. Vea en nuestra página web los que ya estan contribuyendo.

El proceso de traducción también está descrito al completo en www.thegreenbow.es/vpn_local.html.



Contactos

10 Contactos

Información y actualizaciones disponibles en: www.thegreenbow.es
Servicio técnico por e-mail a: support@thegreenbow.es
Departamento de ventas por e-mail a: sales@thegreenbow.es

Index

- Q -

- R -

- S -

Secure, Strong, Simple.

TheGreenBow Security Software